UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- x

                                      :

UNITED STATES OF AMERICA

                                      :

        - v. -   24 Cr. 293 (JGLC)

                                      :

ANTON PERAIRE-BUENO, and
JAMES PERAIRE-BUENO,   :

          Defendants.   :

- x

**THE GOVERNMENT'S OPPOSITION TO
DEFENDANTS ANTON PERAIRE-BUENO AND
JAMES PERAIRE-BUENO'S JOINT PRETRIAL MOTIONS**

                                     MATTHEW PODOLSKY
                                     Chief Counsel to the
                                     Acting United States Attorney
                                     Attorney for the United States,
                                     Acting Under Authority Conferred by
                                     28 U.S.C. § 515

Rushmi Bhaskaran
Jerry Fang
Danielle Kudla
Assistant United States Attorneys

     - Of Counsel -

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

iv

vi

Statutes

Rules

x

PRELIMINARY STATEMENT

The Government submits this memorandum in opposition to defendants Anton Peraire-Bueno and James Peraire-Bueno's joint pretrial motions. (Dkts. 48-56). The defendants' motions seek to dismiss the detailed Indictment by recasting the alleged facts in their own narrative and prematurely contesting the sufficiency of evidence (*see* Dkt. 49); suppress lawfully seized evidence with baseless accusations of law enforcement bad faith (*see* Dkt. 53); compel early production of victim-related information under the guise of a *Brady* claim (*see* Dkt. 51); and obtain information regarding the victims' identities in advance of standard disclosure timelines—much of which, to the extent it is in the Government's possession, has already been provided (*see* Dkt. 55). For the reasons discussed below, the defendants' motions should be denied in their entirety.

The Indictment in this case alleges a meticulously planned fraud scheme, which resulted in the theft of $25 million worth of cryptocurrency (the "Exploit") within seconds from victim cryptocurrency traders (the "Victim Traders"). In the months prior to the theft, the defendants, among other things, drafted a document setting forth the steps needed to successfully execute the Exploit. These steps included identifying and targeting the Victim Traders through deceitful trades; taking advantage of a coding vulnerability to gain early access to private trading information; tampering with the private trading information to their advantage; and concealing their participation in the Exploit through the use of shell companies, intermediary cryptocurrency addresses, foreign cryptocurrency exchanges with limited know-your-customer ("KYC") policies, and a particular blockchain platform designed to help conceal user identities. Following the Exploit, the defendants laundered their millions in ill-gotten gains through privately held cryptocurrency addresses and bank accounts in the name of nondescript limited liability companies

that they established prior to the theft. All the while, the defendants searched online for the very criminal statutes that they are charged with violating.

Each of the defendants' motions should be denied. *First*, the motion to dismiss the Indictment should be denied because the detailed Indictment provides the defendants with thorough notice of the charges against them, far exceeding the legal requirement to proceed to trial. Rather than disputing this, the defendants raise a series of arguments that all miss the mark. Indeed, the vast majority of the defendants' arguments consist of factual disagreements that are more appropriate for a jury address than a pre-trial motion claiming that the Indictment is on its face legally insufficient.   While the defendants claim that the Indictment does not allege a misrepresentation, a deprivation of a traditional property right, or any intent to defraud, the Indictment identifies a series of misrepresentations that the defendants used to orchestrate their scheme to steal millions of dollars of cryptocurrency. The defendants' constitutional challenges fare no better: the defendants' claimed lack of fair notice is not a basis to dismiss the Indictment, especially because the defendants' conduct—including researching the very criminal statutes alleged in the Indictment—show that they knew what they were doing was wrong.

Second, the motion to suppress examines a handful of hyper-specific factual allegations in isolation, contending that each is false based on quibbles with the affiant's word choice or the meaning of those allegations. In doing so, the defendants ignore well-settled precedent rejecting such a divide-and-conquer probable cause analysis and flagrantly disregard the totality of the facts set forth in the 48-page search warrant affidavit. Even more unsettling, the defendants use their reliance on a set of hyper-technical facts to argue that a law enforcement agent intentionally lied to the Magistrate Judge. The search warrant affidavit accurately outlined ample facts setting forth probable cause regarding the defendants' fraudulent scheme. Their word-choice objections to the

terms "no intention," "altered," "arbitrage," or "more obscure tokens" amount to nothing more than their contested view of the facts. In short, the defendants fail to establish that any of their purported "deliberate falsehoods," are, in the context of the affidavit, inaccurate or misleading, never mind material to probable cause. Moreover, their arguments are a far cry from any required showing of intentional bad faith.

Third, the motion to compel the production of purported *Brady* material fundamentally misunderstands the Government's disclosure obligations, ignores the voluminous pre-trial disclosures the Government has already made, and essentially seeks to deputize the Government to affirmatively seek out information for the defense. While the defendants' motion seeks to compel the Government to gather and produce information regarding the Victim Traders' own trading and anonymity practices, the motion fails at the outset because such materials are not exculpatory as to the defendants within the meaning of *Brady* and its progeny. Moreover, the information that the defendants request, to the extent it is in the Government's possession, has already been produced through more than 300,000 pages of Rule 16 discovery, as well as substantive disclosure letters. And to the extent that the defendants seek to compel the Government to search for and gather information not in the Government's possession that may be consistent with defense theories, the law is abundantly clear that there is no such requirement for the Government to do so.

Finally, the defendants' request for a bill of particulars disclosing the names of the victims should be denied. The defendants suggest that the victims' names are necessary for the defendants to investigate their defenses. But a bill of particulars is not a tool to enable a defendant to investigate or conduct discovery—rather, its purpose is to ensure that the defendant is properly advised of the specific acts of which he is accused to avoid prejudicial surprise at trial. There can

be no reasonable dispute that the detailed speaking Indictment and the Government's voluminous pre-trial disclosures more than adequately advise the defendants of the charges against them. And in any event, the Government's disclosures already identify one of the victims and disclose to the defendants the identifying information regarding the other victims known to the Government.

FACTUAL BACKGROUND

As alleged in the Indictment, this case arises from the defendants' theft of approximately $25 million worth of cryptocurrency from Victim Traders. The defendants obtained the Victim Traders' money through their knowledge and manipulation of the process and protocols by which cryptocurrency transactions are validated and added to the Ethereum blockchain. The Indictment provides an overview of many of the facts the Government expects to prove at trial. This factual background section summarizes some of these facts and highlights some areas of disagreement with the defendants' characterization of the facts, but neither this background section nor the Indictment is intended as a complete proffer of the Government's anticipated proof at trial. For the purposes of a motion to dismiss, the allegations in the Indictment must be accepted as true.

A. The Ethereum Network, Maximal Extractable Value, and MEV-Boost

Cryptocurrency is a digital currency in which transactions are verified, and records are maintained, by a decentralized system using cryptography. (Indictment ("Ind.") ¶ 4). Each cryptocurrency transaction is recorded on a public ledger commonly referred to as a "blockchain," which acts as a public accounting record. (*Id.* ¶ 5). "Blocks" are data structures within a blockchain database where transaction information is permanently recorded. (*Id.* ¶ 6).

The crimes alleged in the Indictment relate to the Ethereum network (the "Ethereum Network"), which includes the Ethereum blockchain. (Ind. ¶ 7). "Validators" are a critical participant in the Ethereum Network responsible for checking that new blocks are valid before

they are added to the Ethereum blockchain. (*Id.* ¶ 8). Once selected, a validator has approximately

12 seconds to complete the validation process. (*Id.*). In exchange for validating a new block, a

validator is paid an agreed-upon amount of cryptocurrency that represents a particular portion of

the maximum extractable value ("MEV") (*i.e.*, trading profits) of the transactions that comprise

the new block and other fees, including validator tips. (*Id.*). If a validator attempts to defraud the

Ethereum blockchain or otherwise improperly performs its duties, the validator will be monetarily

penalized. (*Id.*).

When a user conducts a transaction on the Ethereum blockchain, this transaction is not

immediately added to the blockchain. (Ind. ¶ 9). Instead, the pending transaction waits alongside

other pending transactions in the "memory pool" or "mempool," which, notably, is "publicly

visible." (*Id.*). Pending transactions in the mempool are not processed in chronological order, but

rather according the potential MEV that can be obtained by the validators for including, reordering,

or excluding transactions when publishing a new block to the blockchain. (*Id.* ¶ 10.) It is only

after (among other things) pending transactions are structured into a proposed block that is then

validated by the validator that pending transactions are added to the blockchain. (*Id.* ¶ 9). After a

block is published to the blockchain, the block is closed and cannot be altered or removed. (*Id.*).

MEV-Boost is an open-source software "designed to optimize the block-building process

for Ethereum validators by establishing protocols for how transactions are organized into blocks."

(Ind. ¶ 11). Validators who choose to use and rely on the MEV-Boost software as opposed to their

own block-building capabilities outsource the block-building process to a network of "searchers,"

"builders," and "relays." (*Id.* ¶ 12). These participants operate pursuant to protocols designed to

"ensure that each network participant—the searcher, the builder, and the validator—interacts in an ordered manner that maximizes value and network efficiency." (*Id.*).

A searcher is effectively a trader who scans the "public mempool for profitable arbitrage opportunities using automated bots ('MEV Bots')." (Ind. ¶ 13). After identifying a profitable opportunity (that would, for example, increase the price of a given cryptocurrency), the searcher sends the block builder a "proposed 'bundle' of transactions." (*Id.*) "The bundle typically consists of the following transactions in a precise order: (a) the searcher's 'frontrun' transaction, in which the searcher purchases some amount of cryptocurrency whose value the searcher expects to increase; (b) the pending transaction in the mempool that the MEV Bot identified would increase the price of that cryptocurrency; and (c) the searcher's sell transaction, in which the searcher sells the cryptocurrency at a higher price than what the searcher initially paid in order to extract a trading profit." (*Id.*).

A builder receives proposed bundles from various searchers and compiles them into a proposed block that maximizes MEV for the validator. (Ind. ¶ 13). Under the MEV-Boost protocols, the builder then sends the proposed block to a "relay." (*Id.*). When a relay receives the proposed block from the builder, it submits a limited amount of information (*i.e.*, the "blockheader") to the validator concerning, among other things, the payment the validator will receive for validating the proposed block as structured by the builder. (*Id.*). The content of the proposed block (*i.e.*, the complete ordered transaction list), however, remains private. (*Id.* ¶¶ 13-14). Acting in a manner "similar to an escrow account," the relay only releases the otherwise

private transaction information to the validator after the validator has committed "to publishing the block to the blockchain exactly as ordered." (*Id.* ¶ 14).

B. The Defendants' Criminal Scheme

1. The Defendants' Exploit

The defendants orchestrated a scheme to fraudulently steal $25 million worth of cryptocurrency from the Victim Traders on April 2, 2023. (Ind. ¶¶ 1, 23). Their crime involved a series of deceitful trades and lies to profit at the expense of the Victim Traders.

As early as December 2022, the defendants began their scheme by creating a document setting forth their plans for the Exploit (the "Exploit Plan"). (Ind. ¶¶ 16, 21). The Exploit Plan laid out four interconnected stages: "1. The Bait," "2. Unblinding the Block," "3. The Search," and "4. The Propagation." (*Id.* ¶ 21).

In the months that followed, the defendants followed the stages outlined in their Exploit Plan to prepare for and execute the April 2, 2023 Exploit. (Ind. ¶¶ 18-27). Among other things, Anton Peraire-Bueno "searched online for cryptocurrency exchanges with limited 'know your customer' protocols and ways to launder cryptocurrency, including searches for 'how to wash crypto' and 'cefi[1] exchanges with no kyc.'" (*Id.* ¶ 19). He also ran online searches related to Ethereum validator penalties for misconduct—a foreseeable consequence of carrying out the Exploit Plan. (*Id.* ¶ 20). Together, the defendants established a company, Pine Needle Inc. ("Pine Needle"), and opened a corresponding bank account (the "Pine Needle Bank-1 Account") and cryptocurrency account (the "Pine Needle Exchange Account") that would be used for the Exploit and subsequently to launder their ill-gotten gains. (*Id.* ¶¶ 18-19, 31). Between February and March

---

[1] The term "CeFi" refers to a centralized finance exchange, where a central authority manages user funds and transactions. Examples of CeFi exchanges include Binance and Coinbase.

2023, the defendants created 16 Ethereum validators (the "Validators"), which were needed as part of the Exploit, through the use of intermediary cryptocurrency addresses, a foreign-based cryptocurrency exchange, and a privacy layer network designed to conceal user information. (*Id.* ¶ 19). In the days and weeks leading up to the Exploit, the defendants also "tested a series of bait transactions" designed to identify the trading parameters that would cause the Victim Traders' MEV Bots "to propose [trading] bundles to the builder that included the bait transactions." (*Id.* ¶¶ 21-22).

On April 2, 2023—the day of the Exploit—after receiving notification that one of their 16 Validators had been selected to validate a new block (the "Malicious Validator"), the defendants submitted eight transactions (the "Lure Transactions") to the mempool. (Ind. ¶ 24). Based on the defendants' prior bait transactions, they knew the Lure Transactions would cause the Victim Traders' MEV Bots to propose eight bundles that included them. (*Id.*). And that is exactly what happened. In each of these bundles, the Victim Traders purchased substantial amounts of particularly illiquid cryptocurrencies that matched the Lure Transactions (*i.e.*, the frontrun trades) for approximately $25 million of various stablecoins, whose value is pegged to the U.S. dollar or other more liquid cryptocurrencies. (*Id.*). As part of these proposed bundles, the Victim Traders also included a sell transaction in each bundle, whereby the Victim Traders would sell their newly acquired illiquid cryptocurrency immediately after the anticipated execution of the Lure Transaction at a higher price than what they bought it for. (*Id.*). The Victim Traders submitted these proposed bundles to block builders with "coded conditions that the frontrun trades would not be executed unless: (a) the Lure Transactions took place immediately after the frontrun trades; *and* (b) the sell transactions took place immediately after the Lure Transactions." (*Id.*). The block

builders, following the computer code as submitted by the searchers, "submitted the proposed block with the ordered transaction bundles to the Relay." (*Id.* ¶¶ 24-25).

The defendants then used a false digital signature (the "False Signature") to gain premature access to this otherwise private trading information. In particular, the defendants "exploited a vulnerability in the Relay's computer code by sending the Relay [the False Signature] in lieu of a valid digital signature." (Ind. ¶ 26). Based on their prior research and planning, the defendants "knew that the information contained in the False Signature could not be verified for ultimate publication to the blockchain." (*Id.*). Instead, the False Signature was "designed to, and did, trick the Relay to prematurely release the full content of the proposed block to the defendants, including the [Victim Traders'] private transaction information." (*Id.*). Once in possession of this private transaction information, the defendants replaced the Lure Transactions with the transactions that ultimately enabled the defendants to complete the fraud (the "Tampered Transactions"). (*Id.* ¶ 26(b)). The Tampered Transactions sold the same "illiquid cryptocurrencies that the Victim Traders had recently purchased as a result of the Lure Transactions and, for which the defendants *already* held as result of the information gathered through the bait transaction." (*Id.* ¶ 26(b)). Finally, the defendants—using the Malicious Validator—published the "re-ordered block with the Tampered Transactions to the blockchain," which, in effect, stole $25 million worth of cryptocurrency that the Victim Traders parted with based on the Lure Transactions. (*Id.* ¶¶ 26(c), 27).

Against this backdrop, the bait transactions not only ensured that the defendants knew the trading parameters of the Lure Transactions that would cause the Victim Traders to part with their money and propose particular trading bundles, but also that the defendants held the particular cryptocurrency tokens needed to replace the Lure Transactions with the Tampered Transactions

milliseconds later. Likewise, the False Signature not only enabled the defendants to receive premature access to the otherwise private transaction information, but it also provided the defendants with sufficient time to re-order the transactions in the proposed block using the Malicious Validator. Through the defendants' coordinated and deceptive representations using the bait transactions, Lure Transactions, Tampered Transactions, False Signature, and Malicious Validator, the defendants stole the Victim Traders' money. (*See generally* Ind. ¶¶ 23-27).

On April 3, 2023, the day after the Exploit, James Peraire-Bueno emailed a bank representative "asking for a safe deposit box that was large enough to fit a laptop." (Ind. ¶ 28). Two days later, James Peraire-Bueno emailed the website that hosted the open-source code for the Relay ("Website-1") to ask whether Website-1 disclosed certain electronic data that could associate the defendants with the Exploit. (*Id.*) In the following weeks and months, the defendants searched online for, among other things, "how long is us statue [*sic*] of limitations," "wire fraud statute / wire fraud statue [*sic*] of limitations," "fraudulent Ethereum addresses database," "money laundering statue [*sic*] of limitations," "money laundering," "exploit," and "computer fraud abuse act." (*Id.* ¶¶ 29, 32).

2.   The Defendants' Laundering of the Criminal Proceeds

Between April 2023 and June 2023, "foreign law enforcement froze approximately $3 million" of the fraud proceeds, and the defendants were contacted "repeatedly by Victim-1, Victim-1's counsel, or a representative from Ethereum, asking for the return of the stolen funds." (Ind. ¶¶ 30-31). But instead of accepting these invitations to return the stolen funds, "the defendants agreed with each other to launder the proceeds of their fraud." (*Id.* ¶ 30). Shortly after the Exploit, the defendants proceeded to (i) deposit the fraud proceeds into eight separate cryptocurrency addresses that had been funded shortly prior to the Exploit; (ii) transfer the fraud

proceeds from those eight addresses to yet "another privately-held cryptocurrency address"; (iii) convert the fraud proceeds that had not been frozen by foreign law enforcement to DAI, a particular stablecoin; (iv) send the converted DAI to a particular smart contract ("Smart Contract-1") that permits "individuals to borrow and lend DAI in a manner that makes it more difficult to trace on the blockchain"; (v) send the DAI received from Smart Contract-1 to another smart contract ("Smart Contract-2") to swap DAI for USDC, another stablecoin; (vi) send the USDC to the Pine Needle Exchange Account in a series of transactions; (vii) send the fraud proceeds from the Pine Needle Exchange Account to Pine Needle Bank Account-1; (viii) send the fraud proceeds from Pine Needle Bank Account-1 to another recently-opened bank account (the "Birch Bark Bank Account-1"); and (ix) then transfer the fraud proceeds to a separate brokerage account. (*Id.* ¶ 31).

C.   The Charges

The Indictment charges the defendants with conspiring to commit wire fraud (Count One) and wire fraud (Count Two), from December 2022 through May 2024, by agreeing to engage in a scheme to defraud the Victim Traders by making material misrepresentations, including, among other things, through the Lure Transactions and False Signature, in order to fraudulently obtain cryptocurrency. (Ind. ¶¶ 35, 37). The Indictment also charges the defendants with conspiring to commit money laundering (Count Three), from April 2023 through May 2024, by agreeing to launder the fraud proceeds obtained as a result of the Exploit. (*Id.* ¶ 40).

ARGUMENT

I.   The Motion to Dismiss Should Be Denied

The defendants move to dismiss the Indictment based on their disagreement with various facts alleged in the Indictment and the import of those facts. The defendants also contend that the fraud counts must be dismissed as unconstitutionally vague. The defendants' arguments

essentially boil down to premature challenges to the merits of the case and sufficiency of the

Government's anticipated evidence that are not properly raised through a motion to dismiss an

indictment: that is precisely what trials are for. Moreover, the defendants' focus on the "novel"

methods through which they executed the fraud is nothing more than misdirection that ignores the

crux of what the Indictment alleges—a theft. The defendants deceived the Victim Traders into

parting with their money, the defendants took that money, and that the defendants took steps to

conceal their deception and hide their ill-gotten gains. As discussed below, the defendants cannot

establish their entitlement to the "extraordinary remedy" of dismissal of the Indictment, *United

States v. De La Pava*, 268 F.3d 157, 165 (2d Cir. 2001), where—as here—the detailed speaking

Indictment gives sufficient notice of the core criminal conduct alleged.

A. Applicable Law

1. Motion to Dismiss an Indictment

On a pretrial motion to dismiss pursuant to Fed. R. Crim. P. 12(b), the allegations of the

indictment must be taken as true. *See Boyce Motor Lines, Inc. v. United States*, 342 U.S. 337, 343

n.16 (1952); *United States v. Goldberg*, 756 F.2d 949, 950 (2d Cir. 1985).[2] The law is well-settled

that "[a]n indictment returned by a legally constituted and unbiased grand jury . . . if valid on its

face, is enough to call for trial of the charge on the merits." *Costello v. United States*, 350 U.S.

359, 363 (1956). The dismissal of an indictment is an "'extraordinary remedy' reserved only for

extremely limited circumstances implicating fundamental rights." *De La Pava*, 268 F.3d at 165.

"Pursuant to Federal Rule of Criminal Procedure 7, 'the indictment or information must be

a plain, concise, and definite written statement of the essential facts constituting the offense

---

[2] Unless otherwise noted, case quotations omit internal quotation marks, citations, and previous
alterations.

charged.'" *United States v. Vilar*, 729 F.3d 62, 80 n.16 (2d Cir. 2013) (quoting Fed. R. Crim. P. 7(c)(1)). To satisfy this rule, "an indictment need do little more than to track the language of the statute charged and state the time and place (in approximate terms) of the alleged crime." *United States v. Yannotti*, 541 F.3d 112, 127 (2d Cir. 2008). Only in "very rare cases," such as those involving a refusal to answer questions before Congress, must an indictment specify "how a particular element of a criminal charge will be met." *United States v. Stringer*, 730 F.3d 120, 125-26 (2d Cir. 2013) (discussing the unique circumstances of *Russell v. United States*, 369 U.S. 749 (1962)). Otherwise, "[a]n indictment is sufficient if it 'first, contains the elements of the offense charged and fairly informs a defendant of the charge against which he must defend, and, second, enables him to plead an acquittal or conviction in bar of future prosecutions for the same offense.'" *Stringer*, 730 F.3d at 124 (quoting *Hamling v. United States*, 418 U.S. 87, 117 (1974)); *see also Yannotti*, 541 F.3d at 127.

Where a defendant has been given sufficient notice of the charges against him by means of, for example, a charging instrument or discovery, prejudice will not have been shown, and the indictment should stand. *See, e.g.*, *Stringer*, 730 F.3d at 124-25; *Yannotti*, 541 F.3d at 127. Moreover, it is well-settled that, "[u]nless the government has made what can fairly be described as a full proffer of the evidence it intends to present at trial," a facially valid indictment is not subject to challenge based on the quality or quantity of evidence. *United States v. Alfonso*, 143 F.3d 772, 776 (2d Cir. 1998); *see United States v. Williams*, 504 U.S. 36, 54 (1992). To that end, "at the indictment stage, [courts] do not evaluate the adequacy of the facts to satisfy the elements of the charged offense." *United States v. Dawkins*, 999 F.3d 767, 780 (2d Cir. 2021). Rather, "[t]hat

13

is something [courts] do after trial." *Id.* This is consistent with the well-established principle that summary judgment proceedings "do[] not exist in federal criminal procedure." *Id.*

2. Wire Fraud

"The federal mail and wire fraud statutes penalize using the mails or a wire communication to execute 'any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises.'" *United States v. Greenberg*, 835 F.3d 295, 305 (2d Cir. 2016) (quoting 18 U.S.C. §§ 1341, 1343). The "essential elements" of wire fraud are therefore "(1) a scheme to defraud, (2) money or property as the object of the scheme, and (3) use of the . . . wires to further the scheme." *United States v. Saint Clair*, No. 22-2100, 2024 WL 413422, at *4 (2d Cir. Feb. 5, 2024) (summary order).

B. Counts One and Two Sufficiently Allege Violations of Wire Fraud and Conspiracy to Commit Wire Fraud

The 19-page, 43-paragraph Indictment returned in this case amply alleges each of the elements of wire fraud and conspiracy to commit wire fraud and fairly informs the defendants of the charges against which they must defend. The Indictment is sufficient on this ground alone. *See Stringer*, 730 F.3d at 124. Indeed, here, the Indictment provides notice far beyond meeting the basic pleading requirements, setting forth in considerable detail the manner and method in which the defendants' fraud scheme was organized and carried out, the nature of the alleged false statements, the money and property at issue, as well as factual allegations regarding the defendants' fraudulent intent. (Ind. ¶¶ 1-29). The defendants' arguments to the contrary are unavailing as outlined in turn below. Because the Indictment "contains the elements of [each]

offense charged and fairly informs the defendant[s] of the charges against which [they] must defend," *id*., the defendants' motion to dismiss should be denied in its entirety.

1.   The Indictment Adequately Alleges Material Misrepresentations

The defendants argue that the Indictment must be dismissed because it "does not sufficiently allege any material misrepresentation." (Dkt. 49 at 23). This argument is without merit.

As an initial matter, the Indictment tracks the statutory language in alleging that the defendants devised a scheme or artifice to defraud to obtain "money and property by means of false and fraudulent pretenses, representations, and promises."[3] (*See* Ind. ¶¶ 35, 37); 18 U.S.C. 1343. Thus, the fraud counts of the Indictment are legally sufficient.

However, the speaking portion of the Indictment goes far beyond the statutory language in alleging the existence of material misrepresentations in the form of, among other things, the defendants' Lure Transactions and False Signature, both of which the Indictment further describes as necessary steps for the success of the Exploit (*i.e.*, the wire fraud scheme). (Ind. ¶¶ 17, 21-22, 24, 26). The Indictment alleges how the Lure Transactions and False Signature were materially false representations made by the defendants with the intent to obtain the Victim Traders' money. It describes how the defendants "lured the Victim Traders' MEV Bots by proposing at least eight [Lure Transactions]" that based on the defendants' prior tests (*i.e.*, the bait transactions), "the

---

[3] Although the materiality of the misrepresentations is not specifically alleged, it need not be. The Supreme Court found that the concept of materiality is essentially subsumed within the definition of fraud, and thus can be inferred as a required element when a scheme to defraud is charged. *See Neder v. United States*, 527 U.S. 1, 21-25 (1999). Indeed, in *United States v. Klein*, the Second Circuit held that "an allegation of materiality can be inferred from use of the word fraud in the indictment." 476 F.3d 111 (2d Cir. 2007); *see also United States v. Chime*, No. 11 Cr. 244, 2011 WL 3420717, at *2 (N.D. Ohio Aug. 4, 2011) (holding that an indictment that used the words "fraud" and "fraudulent" satisfied the materiality element).

defendants knew would cause the Victim Traders' MEV Bots to propose bundles that included the

Lure Transactions."   (*Id.* ¶ 24).   The Indictment alleges that the Lure Transactions were

misrepresentations because the defendants had no intention of executing them in the Victim

Traders' proposed bundles, but instead, intended to (and did) "replace[] the Lure Transactions"

with the "Tampered Transactions."   (*Id.* ¶¶ 21, 24, 26(b)).[4] As part of this fraud scheme, and

---

[4] Ignoring the allegations that the defendants used the Lure Transactions to induce the Victim
Traders to part with their money in a precise manner essential to the execution of the fraud scheme,
(Ind. ¶¶ 20-22, 26), the defendants contend that there is "no allegation that the Lure Transactions
were not *bona fide* proposed cryptocurrency trades that the defendants honestly offered and
ultimately executed." (Dkt. 49 at 24 & n.18). This argument disregards the totality of the
allegations contained in the Indictment, which clearly outline that the Lure Transactions were
anything but *bona fide* trades, but rather an integral part of the fraud scheme. Namely, at the time
of submission to the mempool, the defendants (i) intended the Lure Transactions to deceive the
Victim Traders into parting with their money, and (ii) knew that the Lure Transactions would never
be executed in the Victim Traders' proposed bundles, but rather swapped with the Tampered
Transactions within milliseconds of achieving the desired market effect.   Even assuming
arguments related to the sufficiency of the Government's evidence are appropriate at this early
stage, which they are not, the mere fact that the Lure Transactions were published to the blockchain
after the alleged crime was complete is irrelevant to the defendants' knowledge and intent
regarding the purpose of the Lure Transactions at the time of their submission to the mempool.
Cf. U.S. ex rel. O'Donnell v. Countrywide Home Loans, Inc., 822 F.3d 650, 658-59, 663 (2d Cir.
2016) (recognizing that conveying a particular intention that is not genuinely held can be a
misrepresentation, noting that a contractual promise to take some action can be fraudulent if the
party making the promise did not intend to keep it "at the time of contract execution"); *see also
United States v. Chanu,* 40 F.4th 528, 541 (7th Cir. 2022) (finding that in the context of "spoofing,"
where a trader places buy or sell orders that the trader actually intends to cancel, with the goal of
manipulating the price of a stock or commodity, constitutes a misrepresentation for purpose of the
wire fraud statute, as the order "signals a trader's intent to buy or sell," but placing such an order
while "obscuring [the] intent to cancel . . . advance[s] a quintessential 'half-truth' or implied
misrepresentation—the public perception of an intent to trade and a private intent to cancel in the
hopes of financial gain"); *see also United States v. Coscia*, 866 F.3d 782, 797-800 (7th Cir. 2017)
(same).   Like in the spoofing cases, the defendants signaled particular trading intentions by
submitting the Lure Transactions to the mempool, while harboring secret intentions to use the
False Signature and the Malicious Validator to replace those very same transactions milliseconds
later with the Tampered Transactions to steal the Victim Traders' money. Absent the fraud
scheme, the Lure Transactions would have been executed in the manner proposed by the Victim
Traders, in accordance with their coded conditions and the Ethereum block-building protocols,
and the alleged crimes would not have occurred.

integral to the replacement of the Lure Transactions with the Tampered Transactions, the

Indictment alleges that the defendants relied upon the False Signature, which "exploited a

vulnerability in the Relay's computer code," giving them premature access to the "private

transaction information" in the proposed block and sufficient time to re-order the transactions to

their advantage. (*Id.* ¶ 26). It was through these coordinated actions that the defendants were

perfectly positioned to (and did) steal $25 million from the Victim Traders. (*Id.* ¶¶ 19, 26-27).

Rather than challenge the legal sufficiency of the Indictment—which they cannot—the

defendants instead prematurely dispute its factual allegations.[5] *See Williams*, 504 U.S. at 54

(noting that it is well-settled that a facially valid indictment is not subject to challenge based on

the quality or quantity of evidence); *United States v. Elie*, No. 10 Cr. 336 (LAK), 2012 WL 383403,

at *1 (S.D.N.Y. Feb. 7, 2021) ("A pretrial motion to dismiss an indictment is not a permissible

vehicle for addressing the sufficiency of the government's evidence.").[6] For example, the

---

[5] For example, the defendants question "the content of the Lure Transactions," "how a validator's signature can be false," "what information a digital signature conveys," "how the signature 'tricked' the relay," why the "information" submitted by the False Signature "could not be verified," and what is the validator's "commitment through a digital signature[.]" (Dkt. 49 at 23-25, 29-33). These questions have no bearing on whether the Indictment sufficiently "contains the elements of the offense charged and fairly informs [them] of the charge against which [they] must defend, and, second, enables [them] to plead an acquittal or conviction in bar of future prosecutions for the same offense." *Stringer*, 730 F.3d at 124; *see also United States v. Raniere*, 384 F. Supp. 3d 282, 298 (E.D.N.Y. 2019) (denying motion to dismiss RICO indictment, noting that "[i]ndictments generally do *not* have to specify evidence or details of how the offense was committed" (emphasis in original)). Although the defendants are not entitled to detailed outlines of the Government's trial proof at this stage, the defendants have received voluminous discovery which addresses many of these questions, including, among other things, electronic returns outlining answers to several of these questions in the defendants' own words.

[6] The Indictment alleges that the defendants "agreed to engage in a scheme to defraud" and "engaged in a scheme to defraud" the Victim Traders "by making material misrepresentations, including, among other things, the Lure Transactions and the False Signature, in order to fraudulently obtain cryptocurrency. (*See* Ind. ¶¶ 35, 37). It does not allege that the defendants omitted information that the defendants had a duty to disclose.

defendants contend that the "Indictment does not say anything about the content of the Lure Transactions." (Dkt. 49 at 23). The Indictment, however, "need[s] to do little more than to track the language of the statute charged and state the time and place (in approximate terms) of the alleged crime." *Yannotti*, 541 F.3d at 127. This Indictment does that and more. To the extent the defendants contest the Government's trial proof or have arguments about the content of the Lure Transactions or their intent when submitting the Lure Transactions, they will have the opportunity to make those arguments to the factfinder at trial. Such factual disputes, however, cannot support dismissal of the Indictment.

Moreover, the defendants' contentions regarding the materiality of Lure Transactions are also questions of fact, not genuine challenges to the legal sufficiency of the Indictment. It is well-established that the issue of materiality must be submitted to the jury. *See United States v. Gaudin,* 515 U.S. 506, 523 (1995); *see also United States v. DeSantis*, 134 F.3d 760, 764 (6th Cir. 1998) ("[U]nless no reasonable mind could find a statement or omission to be material, a criminal trial court *must* submit the issue to the jury." (citing *Gaudin*, 515 U.S. at 511) (emphasis in original)); *United States v. Gatto*, 295 F. Supp. 3d 336, 349-50 (S.D.N.Y. 2018) (same).

Similarly, questions regarding whether a statement, such as a Lure Transaction or the False Signature, is false or misleading, (*see* Dkt. 49 at 23-25), are also factual matters to be determined by the jury. *See United States v. Phillips*, 690 F. Supp. 3d 268, 291-92 (S.D.N.Y. 2023) (denying motion to dismiss wire fraud counts noting that whether a statement or omission is false or misleading goes to the sufficiency of the evidence to be evaluated by the jury); *United States v. Khalil*, No. 13 Cr. 386, 2014 WL 1599943, at *2 (E.D.N.Y. April 21, 2014) (same) (collecting cases); *see also United States v. Fanta*, No. 04 Cr. 1253, 2005 WL 3455755, at *2 (S.D.N.Y. Dec. 16, 2005) (denying motion to dismiss indictment because defendant's argument that alleged

18

statements were not, in fact, false raised dispute about facts to be proven at trial). Here, the

defendants' arguments concerning the precise contours of how the Lure Transactions and False

Signature are false are challenges to the Government's proof, which is premature at this stage.[7]

Finally, the defendants' contention that the False Signature "cannot have been a material

misrepresentation within the meaning of the wire fraud statue [*sic*]" because it had "no role in

causing the alleged victims to part with their money," (Dkt. 49 at 25), is wrong on the facts and

the law. As to the facts, the defendants' assertion that the False Signature failed to play a role in

obtaining money from the Victim Traders is simply contrary to the allegations in the Indictment,

which must be accepted as true. As alleged, the False Signature "exploited a vulnerability in the

Relay's computer code" and caused the Relay to "prematurely release the full content of the

proposed block to the defendants, including the [Victim Traders'] private transaction information."

(Ind. ¶ 26). As such, far from playing "no role" in the fraud, it was integral to the Exploit. (*Id.*).

And as noted above, to the extent that the defendants wish to challenge the role played by the False

Signature in the scheme, they will have their opportunity at trial. *See United States v. Eisenberg*,

23 Cr. 10 (AS), 2023 WL 8720295, at *6 (S.D.N.Y. Dec. 18, 2023) (denying motion to dismiss a

wire fraud charge where the defendant contended that his conduct was "fully permitted" by the

---

[7] As alleged, the defendants were responsible for creating and deploying the Lure Transactions and the False Signature, which were both essential to the success of the Exploit. (Ind. ¶¶ 17, 21-22, 24-26). The defendants suggest without any supporting authority that they cannot be held responsible for any wrongdoing because the crime was "executed through automated code without the counterparties even interacting" in a manner permitted by open-source code. (*See* Dkt. 49 at 2, 6, 13 (noting that smart contracts execute "based on the conditions written within the contract's code" rather than relying "on humans to interpret")). Despite their contentions to the contrary, (Dkt. 49 at 14 n.8), the defendants appear to be asserting a "code is law" defense—meaning that if an action is permitted by the code, even in the event of a vulnerability, bug, or glitch in the code, that action should be considered permissible. To the extent they believe this defense is relevant, such an evaluation is more appropriate for motions *in limine* and, only if thereafter deemed admissible, an argument for the jury.

computer code operating a particular cryptocurrency exchange and therefore, he "deceived no one"; finding "[t]hat might be what the facts show at trial[,] [b]ut for present purposes, the indictment certainly alleges 'a scheme to engage in some form of deception' in connection with [the defendant's] trades and his taking of $110 million in crypto[.]'").

In addition, the defendants' further contention that the False Signature "had no role in causing the alleged victims to part with their money" because the Relay did not have "any contact with the allegedly lost cryptocurrencies," (Dkt. 49 at 25), is contrary to law. The Second Circuit has held that to prove wire or mail fraud, "the party whose money or property is the object of the scheme [need not be] the same party whom a fraudster seeks to deceive." *Greenberg*, 835 F.3d at 306; *United States v. Weigand*, 482 F. Supp. 3d 224, 237 (S.D.N.Y. 2020), *as corrected* (Sept. 2, 2020) ("Five courts of appeals, including the Second Circuit, have concluded that the wire fraud statute does not 'require convergence between the parties intended to be deceived and those whose property is sought in a fraudulent scheme.'" (quoting *Greenberg*, 835 F.3d at 306-07)). The Circuit thus has squarely rejected the convergence argument advanced by the defendants.

The Indictment properly alleges that the defendants engaged in a scheme "to fraudulently obtain approximately $25 million worth of cryptocurrency from [the Victim Traders]." (Ind. ¶ 1). It is irrelevant that one of the means through which the defendants committed this fraud was to make a false representation to the Relay as opposed to the Victim Traders. *See United States v. Martinez*, 22 Cr. 251 (LJL), 2023 WL 2118081, at *3 (S.D.N.Y. Feb. 17, 2023) (rejecting claim that false representations made to the U.S. Small Business Administration in order to obtain money

20

from an insurance company and the Federal Reserve Bank of San Francisco were "too attenuated to constitute wire fraud").

Under *Loughrin v. United States*, 573 U.S. 351 (2014), the Supreme Court held that the Government must show "a relational component"—that the relationship between the end of achieving money or property from the bank and the means of making a false statement to a third party "is something more than oblique, indirect, and incidental." *Id.* at 362-63. In the bank fraud context, the Supreme Court articulated that the "'by means of' language [in the bank fraud statute] is satisfied when . . . the defendant's false statement is the mechanism naturally inducing a bank (or custodian of bank property) to part with money in its control." *Id.* at 363. Here, the Indictment alleges such a causal relationship. Specifically, it alleges that defendants sent the False Signature to the Relay to "trick the Relay to prematurely release the full content of the proposed block to the defendants, including the [Victim Traders'] private transaction information," which the defendants tampered with to their advantage and thereby obtained millions of dollars of worth of cryptocurrency from the Victim Traders—all of which occurred within seconds. (Ind. ¶¶ 1, 8, 26).

The Sixth Circuit's decision in *United States v. Palma*, 58 F.4th 246 (6th Cir. 2023), is instructive. The defendant in that case conspired to falsify test results for a new diesel engine and to market the engine as environmentally friendly and "best in class," with the ultimate object of obtaining money from the consumers who purchased the cars in which the engines had been installed. *Id.* at 247. The district court granted a motion to dismiss on the ground that "there was an insufficient causal nexus between Palma's conduct and customers being induced to purchase vehicles." *Id.* at 249. On appeal, the Sixth Circuit reversed, finding that the indictment had alleged "a sufficient causal nexus between the conduct of Palma and coconspirators and a deprivation of property." *Id.* at 249-51. The court emphasized, among other things, that the decision came at the

21

pleading stage, such that "the government need only allege facts showing that the conspiracy as a whole had the object of using deception to deprive consumers of property," and the court did "not test the evidence behind [the government's] claims." *Id.* at 250 (distinguishing *Kelly v. United States*, 590 U.S. 391 (2020), because "*Kelly* took place in post-conviction proceedings, whereas Palma challenges an indictment," and the "property loss [in *Palma*] is much more significant than the loss in *Kelly*[, where the Supreme Court held that realigning traffic lanes for political reasons failed to meet the property requirement for fraud,] and much more connected with the alleged scheme").

The *Palma* court also distinguished *Berroa*, the primary case relied upon by the defendants, (Dkt. 49 at 25), in which the First Circuit reversed convictions for mail fraud based on *Loughrin*. *Palma*, 58 F.4th at 250-51. In *Berroa*, the defendants were charged with mail fraud based on having falsified test scores to obtain medical licenses, which they then used "in the ensuing years after becoming licensed" to "practice[] medicine for profit." 856 F.3d 141, 152 (1st Cir. 2017). The First Circuit found an insufficient causal nexus between the falsified test scores and the profit, noting that "the defendants' alleged fraud in obtaining their medical licenses cannot be said to have 'naturally induced' healthcare consumers to part with their money *years later*." *Id*. at. 150-51 (emphasis added). In distinguishing *Berroa*, the Sixth Circuit noted that "where the purpose of fraudulently obtaining medical licenses was to practice medicine, the goal of 'cycle beating' and falsely inflating the engines' performance"—the deception alleged in *Palma*—was "to induce customers who otherwise would not have bought the vehicles to do so." *Palma*, 58 F.4th at 251. The court continued that, "[u]nlike *Berroa*, the case at bar is clearly about property. And it is

plausible that the scheme's goal was not merely to deceive regulators but also to sell the resulting products to consumers." *Id.*

Like *Palma*, the instant case is, without question, a case "about property"—the millions of dollars' worth of Victim Traders' cryptocurrency that flowed to the defendants through their use of the Lure Transactions and the False Signature. *See Palma*, 58 F.4th at 251. And it is well beyond "plausible"—indeed, it is the only logical conclusion to be drawn—that the goal of the defendants' submission of the False Signature to the Relay was not merely to deceive the Relay for their own sake, but to put the defendants in a position to steal the Victim Traders' cryptocurrency. *See id*. Indeed, unlike in *Berroa*, where years passed between the false statements and the profit, here, the defendants' execution of the Lure Transaction and the False Signature and efforts to obtain the Victim Traders' cryptocurrency were nearly contemporaneous. (Ind. ¶ 8 ("a validator has approximately 12 seconds to complete the validation process"). The defendants' claim that the False Signature "could have had no role in causing the alleged victims to part with their money," (Dkt. 49 at 25), strains credulity. As in *Palma*, the conspiracy as a whole had the object of using deception to deprive the victims of property. The defendants' arguments parsing each step of the fraud scheme as though they were not integral to the success of the scheme as a whole cannot be squared with the law and the facts.

For the foregoing reasons, the defendants' attempts to contend that the detailed Indictment fails to allege a single false statement or misrepresentation should be rejected, and their motion to dismiss should be denied.

2. The Indictment Adequately Alleges a Scheme to Defraud Victims of Money or Property

Counts One and Two properly allege that the defendants conspired to and schemed to defraud the Victim Traders by "making material misrepresentations, including, among other things, the Lure Transactions and the False Signature, *in order to fraudulently obtain cryptocurrency*." (Ind. ¶¶ 35, 37 (emphasis added)). The charges track the statutory language of 18 U.S.C. §§ 1349 and 1343, respectively, and allege that the objective of the scheme to defraud was to "obtain money and property." (*Id.* ¶¶ 65, 67); *see, e.g.*, *United States v. Bankman-Fried*, 680 F. Supp. 3d 289, 307 (S.D.N.Y. 2023) (holding that indictment alleging misappropriation of "'billions of dollars' of . . . funds, including both fiat deposits and cryptocurrency assets" "plainly constitute[s] both 'money' and 'property' within the meaning of Section 1343"); *Eisenberg*, 2023 WL 8720295, at *6 (holding that indictment alleging misappropriation of $110 million in cryptocurrency sufficiently alleged a wire fraud violation).

Aiming their arguments at a strawman indictment rather than the Indictment returned by the grand jury, the defendants move to dismiss the wire fraud counts, arguing that the Indictment fails to allege the deprivation of a "traditionally recognized, enforceable property right." (Dkt. 49 at 26). The defendants assert that the Victim Traders did not lose money based on the alleged fraud scheme because they had already "trad[ed] away their cryptocurrencies with no guarantee that their manipulative strategy would yield profits," and therefore, the Victim Traders "forfeited" their property rights for an "expectation of future financial gain dependent on events outside of their control." (Dkt. 49 at 27-28). Following the defendants' argument to its logical conclusion, scenarios where victims part with their money based on false promises of "future financial gain" (*i.e.*, the basis for countless fraud schemes, such as romance scams falsely promising gold and

24

riches upon an initial investment, *Ponzi* schemes falsely promising lucrative returns, or any scheme

for that matter where a defendant directs a victim to give their money to an intermediary based on

false promises knowing the defendant would ultimately obtain that money) would fall outside the

purview of wire fraud. The defendants' argument cannot be squared with the facts or the law.

Contrary to the defendants' assertion, the Indictment does not allege a case about a scheme

to defraud victims of *expected* profits. This is a case about stolen money belonging to the Victim

Traders. The Victim Traders had millions of dollars' worth of cryptocurrency in their wallets,

which the defendants obtained through a coordinated series of misrepresentations. (Ind. ¶¶ 16-27).

The Victim Traders parted with approximately $25 million in cryptocurrency as a direct result of

the defendants' Lure Transactions. (*Id.* ¶ 24). The defendants knew these deceitful trades would

be (and were) replaced just seconds later with the Tampered Transactions using the False Signature

and the Malicious Validator—and as a result, the defendants knew they would (and did) walk off

with the Victim Traders' money. (*Id.* ¶¶ 24 ("The Lure Transactions did, in fact, cause the Victim

Traders to propose eight bundles that included the Lure Transactions . . . . In each of these eight

bundles, the Victim Traders effectively bought substantial amounts of particularly illiquid

cryptocurrencies (the frontrun trades) . . . for approximately $25 million of various stablecoins"),

26 ("In effect, the Tampered Transactions drained the particular liquidity pools of all the

cryptocurrency that the Victim Traders had deposited as a result of their frontrun trades.")).

As alleged, the object of the defendants' fraud scheme was to obtain the Victim Traders'

money via misrepresentations—the core object of the wire fraud statute. *See, e.g.*, *United States

v. Males*, 459 F.3d 154, 158-59 (2d Cir. 2006) ("The requirement under § 1343 that the defendant

devise a scheme or artifice for obtaining money or property is satisfied where a defendant

fraudulently obtains the use of another person's money or property for a period of time, using it

for his own personal profit, and depriving the owner of the ability to do so."); *United States v. Andrew*, 22-1749, 2024 WL 4297474, at *2 (2d Cir. Sept. 26, 2024) (summary order) (affirming wire fraud conviction where object of the scheme was to steal money belonging to charter schools); *United States v. Tuzman*, 21-2229, 2024 WL 1173044, at *3 (2d Cir. Mar. 19, 2024) (summary order) (affirming wire fraud conviction where the defendants' scheme involved "knowingly sending false financial statements to [victim] investors precisely to deprive them of their money").

The defendants rely heavily on *United States v. Henry*, 29 F.3d 112 (3d Cir. 1994). *Henry* involved a bid-rigging scheme whereby the defendants were convicted of mail fraud for giving one bank confidential information about bids from other banks. *Id.* at 113. The fraud claims focused on the "alleged corruption of the process by which" the bids were selected—not the fraudulent obtaining of money. *See id.* at 113 (quoting the § 1343 indictment language, "'[the defendants] . . . defrauded the other banks bidding . . . in that they denied these other bidding banks a fair and honest opportunity to receive this public money' or 'a fair and honest opportunity to bid on' it"). As alleged in *Henry,* the issue was whether competing banks had a recognizable property interest in a fair bidding process. *See id.* at 115. By contrast, the Indictment alleges that the object of the defendants' fraud scheme was not the "corruption" of the MEV-Boost block-building process, but rather obtaining the Victim Traders' cryptocurrency—money which the Victim Traders already possessed, and which the defendants' misrepresentations caused them to part with. (Ind. ¶¶ 24-26, 35, 37 ("[The defendants] engaged in a scheme to defraud the Victim Traders . . . in order to fraudulently obtain cryptocurrency.")). The manipulation and tampering with the block-

building process was not the object of the fraud scheme, but simply the means to obtain what the

defendants truly sought—the Victim Traders' money.[8]

Accordingly, and because the Indictment alleges a scheme to deprive the Victim Traders

of money or property (*i.e.*, the millions worth of cryptocurrency they parted with as a direct result

of the defendants' misrepresentations), the claim that the Indictment fails to allege the "deprivation

of a traditionally recognized, enforceable property right," (Dkt. 49 at 26), is without merit.

3.   The Indictment Adequately Alleges the Defendants' Intent to Defraud

Finally, the defendants argue that the Indictment should be dismissed because it does not

allege a scheme to defraud because the Victim Traders received the "benefit of their bargain."

(Dkt. 49 at 28). This argument is not only premature but disregards the Indictment allegations.

In order to prove a "scheme to defraud," the Government must show "that the defendant

possessed a fraudulent intent." *Greenberg*, 835 F.3d at 305-06. However, "the Government need

---

[8] Setting aside *Henry*, the other cases relied upon by the defendants are equally unavailing and inapplicable to this case. (Dkt. 49 at 26). *See United States v. Pierce*, 224 F.3d 158, 160, 164, 168 (2d Cir. 2000) (reversing wire fraud conviction where government failed to elicit proof at trial that the Canadian government imposed duties or taxes on the importation of liquor, which based on the indictment, was the object of the defendant's fraud scheme); *United States v. Adler*, 186 F.3d 574, 575, 577-78 (4th Cir. 1999) (affirming judgment of acquittal following wire fraud conviction after the court found the defendant's oral promise to repay a debt owed to the victim with anticipated settlement proceeds belonging only to the defendant did not deprive the victim "of anything that [the victim] actually owned"); *United States v. $52,037.96*, 14 Civ. 591, 2015 WL 5601848, at *7-8 (D. Conn. Sept. 23, 2015) (granting motion to dismiss of a civil *in rem* action involving an honest services wire fraud complaint where the alleged harm was a "manufacturer's interest in controlling future market conditions," but the manufacturer was not even a party to the transaction at issue); *Pharmacare v. Caremark*, 965 F. Supp. 1411, 1417 (D. Haw. 1996) (finding that plaintiffs in a civil RICO action failed to allege mail and wire fraud claims as predicate acts where the alleged property rights were "the right to a level playing field" and "the right of the physicians' patients to honest services"); *Roitman v. N.Y.C. Transit Auth.*, 704 F. Supp. 346, 349 (E.D.N.Y. 1989) (finding that expectation of employment as a teacher was not a cognizable property right in a civil rights and RICO action against police officers for an alleged false arrest where there were insufficient facts to suggest that the plaintiff had a "legitimate claim of entitlement" to that right such as a prior teaching job).

not prove that the victims of the fraud were *actually* injured, but only that defendants *contemplated* some actual harm or injury to their victims." *Id.* at 306 (emphasis in original). "Such harm is apparent where there exists a discrepancy between benefits reasonably anticipated because of the misleading representations and the actual benefits which the defendant delivered, or intended to deliver." *United States v. Jabar*, 19 F.4th 66, 76-77 (2d Cir. 2021) (reversing district court's post-verdict judgment of acquittal and finding evidence of defendant's fraudulent intent).

As a threshold matter, the question of whether the Victim Traders received "the benefit of their bargain" as relevant to the defendants' fraudulent intent a question of fact for the jury. *United States v. Tanner*, 17 Cr. 61 (LAP), 2018 WL 1737235, at *6 (S.D.N.Y. Feb. 23, 2018) (noting that the question concerning the defendant's fraudulent intent "is a question of fact for the jury") (collecting cases). Notably, the cases relied upon by the defendants—*United States v. D'Amato*, 39 F.3d 1249 (2d Cir. 1994), *United States v. Starr*, 816 F.2d 94 (2d Cir. 1987), and *United States v. Shellef*, 507 F.3d 82 (2d Cir. 2007)—are post-trial challenges to the sufficiency of evidence. Here, there has been no trial, no evidence has been offered, and the sole issue before the Court is the facial validity of the Indictment.

When turning to the allegations in the Indictment—which must be accepted as true—the Victim Traders in no way got "precisely what they bargained for in their trades." (Dkt. 49 at 28). To the contrary, the Indictment alleges that the Victim Traders proposed bundles that were materially different than what were published to the blockchain. (Ind. ¶¶ 24, 27). In particular, the Victim Traders expected that their frontrun trades would only be executed if the Lure Transactions were executed immediately thereafter, *and* the sell transactions took place

28

immediately after the Lure Transactions. (*Id.*). [9] As alleged—it was the sequential execution of

all three trades (*i.e.*, the frontrun transaction, the Lure Transaction, and the sell transaction) that

was essential to the Victim Traders. Instead, as part of the fraud scheme, the defendants used

(i) the Lure Transactions to induce the Victim Traders to part with their money in a particular

manner, (*id.*); (ii) the False Signature to gain premature access to the Victim Traders' private

transaction information, (*id.* ¶ 26); and (iii) the Malicious Validator to replace the Lure

Transactions with the Tampered Transactions and publish the re-ordered block to the blockchain

(*id.* ¶¶ 23, 25, 26(b), 27).

The Indictment does *not* allege that the Victim Traders bargained for their frontrun trades

to be executed even though the Lure Transactions—an essential transaction in the Victim Traders'

proposed bundles—were not. Given this sequence of events, it is unclear how the defendants can

plausibly argue that the Victim Traders got the "benefit of the bargain" in any manner, let alone

one that suggests that the defendants did not "contemplate[] harm" to the Victim Traders as part

of their fraud scheme. *See Jabar*, 19 F.4th at 76. Indeed, as alleged, the objective of the fraud

scheme was to steal the Victim Traders' money—which they successfully did.

The defendants' reliance on *D'Amato*, *Starr*, and *Shellef*, (Dkt. 49 at 28), is misplaced given

that they all turn on facts readily distinguishable from this case. In *D'Amato*, the defendant, who

was the brother of then-Senator Al D'Amato, was retained by an executive at a company for the

purposes of lobbying his brother on issues of legislative interest to the company. 39 F.3d at 1252.

---

[9] The defendants pose evidentiary questions regarding the contours of how the defendants' fraud scheme successfully counteracted the Victim Traders' coding conditions. (Dkt. 49 at 29 n.21). Once again, a pretrial motion to dismiss is not the permissible vehicle for addressing such sufficiency of evidence arguments—that is the purpose of trial and the "proof beyond a reasonable doubt" standard. *See Boyce Motor Lines, Inc.*, 342 U.S. at 343 n.16.

Because it was potentially embarrassing to the company—although not illegal—to pay the defendant to gain access to his brother, the executive asked the defendant to submit invoices for his work that (1) omitted the defendant's name, and (2) purported to be for different services, namely a series of "reports" the defendant never actually intended to create. *Id.* at 1254, 1259. The Government charged the defendant with fraud, on the theory that the fake invoices he submitted at the behest of a corporate executive defrauded the company, the defendant was convicted at trial, and the Second Circuit reversed, holding that a person hired to perform services for a corporation "cannot be found to intend to harm a corporation or its shareholders through otherwise lawful misleading conduct if he or she follows the instructions of an appropriate corporate agent who appears to be unconflicted and acting in good faith." *Id.* at 1258. As the Court continued, the Government's fraud theory could not be extended to "innocent provider[s] of services . . . unaware of the effect of [their] actions." *Id.* at 1261.

Unlike in *D'Amato*, the defendants are not alleged to be "innocent provider[s] of services . . . unaware of the effect of [their] actions," 39 F.3d. at 1261, and their conduct cannot be described as "otherwise lawful" activity done pursuant to instructions "of an appropriate corporate agent . . . acting in good faith," *id.* at 1258. Instead, the defendants are alleged to be orchestrators of a criminal scheme whose goal was to defraud the Victim Traders of their money. Indeed, unlike *D'Amato*, where the trial evidence established that the defendant had little experience with the victim company or reason to infer criminal motives for the requested fake invoices, here the Government has alleged that the defendants—highly educated in mathematics and computer

30

science and experienced in cryptocurrency trading—plainly understood both the fraudulent nature

of their conduct and the potential effects of that conduct on the Victim Traders. (Ind. ¶¶ 1, 16-27).

The facts of *Shellef* and *Starr* are equally distinguishable. *Shellef* is a right-to-control theory

fraud case where the "property" involved the right to make informed economic decisions, not, as

alleged here, the fraudulent obtainment of the victim's money. In *Shellef*, the defendant

misrepresented to manufacturers that he intended to export a purchased industrial chemical product

(thus rendering the sale excise-tax-free), when in fact, he intended to sell the product domestically.

507 F.3d at 90-93. In one of the two wire fraud theories asserted in the indictment, it was alleged

that the defendant had deprived the victim of the "the right to define the terms for the [contractual]

sale of its property," but failed to further allege that the defendant's misrepresentation had

"relevance to the object of the contract." 507 F.3d at 107, 109. The *Shellef* court found the wire

fraud charge was insufficient because there was no indication that the misrepresentation was an

"essential element" of the bargain between the two parties—an issue not present here where the

Indictment alleges that the defendants' misrepresentations in the form of the Lure Transactions

were an essential component of the Victim Traders' proposed bundles. *Id.* at 109.[10]

In *Starr*, the owners of a bulk mailing company schemed to conceal higher rate mailings

from customers in lower rate bulk mailings without paying the additional postage to the postal

service or refunding their customers' excess postage payments. 816 F.2d at 95. The defendants

"represented that funds deposited with them would be used only to pay for their customers' postage

---

[10] Notably, and more similar to this case, the second wire fraud theory, which the *Shellef* court found legally sufficient, rested on the allegation that the same misrepresentation fraudulently induced the victim to sell the product without the required "excise tax," which deprived the victim of "money" that "was owed to it"—not a deprivation of valuable economic information. 507 F.3d at 109. But because the jury's verdict rested on "multiple theories of conviction," only one of which was valid, the court overturned the conviction. *Id.* at 107, 110.

fees," but upon defrauding the postal service, defendants sent fraudulent receipts to their customers and appropriated the remainder of the funds for their own use. *Id.* at 99. The court concluded that because the customers' mail was delivered on time to the correct location, whatever harm there was did not "affect the very nature of the bargain itself." *Id.* at 98. At most, the government's evidence showed defendants' intent to deceive or induce customers into the transaction but not a fraudulent intent. *Id.* at 100. As noted in the concurring opinion, the Postal Service was defrauded, but not the defendants' customers—and the government "simply indicted the defendants for defrauding the wrong party." *Id.* at 102 (Newman, J., concurring).

The essential thread running through *Shellef* and *Starr* is that the alleged victims received the benefit of their bargain, and thus, absent actual harm suffered by the victims, there was insufficient evidence that the defendants contemplated harm to the victims as part of the fraud scheme. This is not the pattern alleged in the Indictment. By contrast, the Victim Traders suffered actual harm—approximately $25 million worth of stolen money—because, among other things, the defendants deliberately replaced the Lure Transactions, which were an essential component of the Victim Traders' proposed bundles, with the Tampered Transactions. This was clearly an artifice used by the defendants to take the Victim Traders' money through fraud, and exactly the kind of conduct prohibited by the wire fraud statute. (Ind. ¶¶ 23-24, 26). *See Jabar*, 19 F.4th at 76 ("Fraudulent intent may be inferred when the necessary result of the actor's scheme is to injury others.").

The Indictment further alleges that the defendants took countless steps to conceal their identity, all of which are indicative of fraudulent intent. Specifically, the defendants established a series of Ethereum validators, including the Malicious Validator used in the Exploit, "through the use of shell companies, intermediary cryptocurrency addresses, foreign exchanges, and a privacy

32

layer network," (Ind. ¶ 17); "searched online for cryptocurrency exchanges with limited [KYC] protocols and ways to launder cryptocurrency, including searches for 'how to wash crypto' and 'cefi exchanges with no kyc,'" (*id.* ¶ 19); contacted Website-1, which hosted the source code for the Relay and was accessed by Anton Peraire-Bueno prior to the exploit, "asking whether Website-1 provides censored IP addresses for access logs[,]" (*id.* ¶ 28); refused repeated requests by "Victim-1, Victim-1's counsel, or a representative from Ethereum" to "return the stolen funds," (*id.* ¶ 30); and even after "foreign law enforcement froze approximately $3 million . . . of the fraud proceeds," took elaborate steps to off-ramp their ill-gotten gains through privately held cryptocurrency addresses, various cryptocurrency swaps, and multiple, smaller transactions designed to evade further detection, (*id.* ¶ 31).

When taken as true, the Indictment allegations more than adequately describe facts supporting the defendants' fraudulent intent to defraud the Victim Traders of approximately $25 million. Because there is no deficiency in the Indictment's allegations, the defendants' motion to dismiss on those grounds should be denied.

C. The Defendants' Vagueness Challenges Should Be Denied

The defendants next claim that Counts One and Two should be dismissed because they are unconstitutionally vague—namely, that the Indictment is vague because it fails to sufficiently allege a false or misleading statement in a manner that provides fair notice, (Dkt. 49 at 29-33), and because the wire fraud theory is (i) vague as applied to them; and (ii) a "novel construction" of the statute. (Dkt. 49 at 10-19). The defendants' vagueness challenges are meritless.

1. Applicable Law

"The void-for-vagueness doctrine springs from the Fifth Amendment's due process clause," *United States v. Houtar*, 980 F.3d 268, 273 (2d Cir. 2020), and "requires that a penal

statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement." *United States v. Morrison*, 686 F.3d 94, 103 (2d Cir. 2012). "The doctrine addresses concerns about (1) fair notice and (2) arbitrary and discriminatory prosecutions." *United States v. Halloran*, 821 F.3d 321, 338 (2d Cir. 2016). Under the fair notice prong, the question is "whether the statute, either standing alone or as construed, made it reasonably clear at the relevant time that the defendant's conduct was criminal." *Id.*

"When a vagueness challenge alleges lack of notice, the relevant inquiry is whether the statute presents an ordinary person with sufficient notice of what conduct is prohibited." *Houtar*, 980 F.3d at 273. "This requirement assures that statutes do not lull the potential defendant into a false sense of security, giving him no reason even to suspect that his conduct might be within its scope." *Id.* "Statutes need not, however, achieve meticulous specificity, which would come at the cost of flexibility and reasonable breadth." *Id.*; *accord United States v. Farhane*, 634 F.3d 127, 139 (2d Cir. 2011). Notably, "[t]here are three related manifestations of the fair warning requirement": the vagueness doctrine; the rule of lenity, which "ensures fair warning by so resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered"; and a bar on courts "applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope." *United States v. Lanier*, 520 U.S. 259, 266 (1997).

2. Discussion

      i. The Allegations in the Indictment are Not Unconstitutionally Vague

The defendants also contend that the Indictment is void for vagueness because it does not provide fair notice to the defendants as to any alleged false or misleading statement. (Dkt. 49 at 30). The defendants' argument fails on both the facts and law.

As outlined above in Section I(B)(1), the speaking portion of the Indictment goes far beyond the required statutory language in alleging the existence of material misrepresentations in the form of, among other things, the defendants' Lure Transactions and False Signature, both of which the Indictment further describes as necessary steps for the success of the Exploit (*i.e.*, the wire fraud scheme). (Ind. ¶¶ 17, 21-22, 24, 26). Specifically, the Indictment alleges how the Lure Transactions and False Signature were materially false representations made by the defendants with the intent to obtain the Victim Traders' money. The allegations sufficiently apprise the defendants of the charges they must defend at trial.

The defendants' reliance on *United States v. Pirro*, 212 F.3d 86 (2d Cir. 2000), *Russell v. United States*, 369 U.S. 749 (1962), and *United States v. Curtis*, 506 F.2d 985 (10th Cir. 1974), (Dkt. 49 at 20, 30, 32), to contend otherwise is misplaced.

In *Pirro*, the Second Circuit ordered dismissal of a count in an indictment that charged the defendant with having failed to disclose his ownership interest in a company on a tax return. It reasoned that the government had merely alleged the defendant's omission of an "ownership interest," rather than his "share ownership," and that it was not clear that defendant had a legal duty to disclose an ownership interest other than share ownership. 212 F.3d at 93. It therefore held that the defendant "was not adequately informed of the nature of the accusation against him,

35

as is his right under the Sixth Amendment" because "[t]he indictment allege[d] the omission of a fact that [the defendant] might not have been required to report." *Id.* at 95.

In *Russell*, the Supreme Court ruled that the indictment was insufficient to put the defendants on notice of the charges against them. 369 U.S. at 771. There, the defendants were convicted, pursuant to 2 U.S.C. § 192, of refusing to answer certain questions posed by a congressional subcommittee. *Id.* at 752. The indictment, however, failed to identify the subject matter under congressional subcommittee inquiry. *Id.* at 752-53. This, the Supreme Court concluded, was a constitutional violation because the underlying charge depended on the subject-matter of the questions. *Id.* at 764, 768 ("[T]he very core of criminality under 2 U.S.C. § 192 . . . is pertinency to the subject under inquiry of the questions which the defendant refused to answer.").

Likewise, in *Curtis*, the Tenth Circuit held that the barebones indictment was so vague that "the grand jury may have had a concept of the scheme essentially different from that relied upon by the government before the trial jury." 506 F.2d at 989. There, the defendant founded a dating service. *Id.* at 986–87. All the indictment alleged was that the service was a sham—it provided no detail as to why it was a sham. *See id.* at 988-89. Thus, on appeal, the court concluded that the indictment was unconstitutionally vague because it contained no language about *what* conduct formed the scheme. *See id.* at 992.

All three cases are easily distinguishable from the Indictment in this case, which outlines the fraud scheme in ample detail, including, among other things, (i) relevant background concerning the Ethereum Network, including the roles of the Ethereum network participants and the block-building process and protocols established by the MEV-Boost system that the defendants are alleged to have manipulated and tampered with (Ind. ¶¶ 1, 4-15), and (ii) numerous actions taken by the defendants in furtherance of their fraud scheme, including countless steps to conceal

their identity (*id.* ¶¶ 16-29). The Second Circuit has already distinguished *Pirro* and *Russell* as

being among the "very rare cases in which an indictment that tracked the statutory language and

furnished the pertinent dates was held insufficient." *Stringer*, 730 F.3d at 125-27. The Circuit

clarified that both cases fell into a "less-common category" of cases that involved charges of

criminal falsity, where the "specification of how a particular element . . . will be met (as opposed

to categorical recitation of the element) is of such importance to the fairness of the proceeding that

it must be spelled out in the indictment." *Id.* at 126-127. Similarly, *Curtis*—a 50-year-old, non-

binding precedent—is equally unavailing here, where it is clear that the Indictment does not just

merely allege that the defendants' actions were fraudulent without any further detail. Here, in

sharp contrast to *Curtis*, the defendants' fraud is extensively outlined in the Indictment.

Simply put, the issue of sufficient notice is not implicated here. This Indictment does not

rely on something akin to an unalleged duty to disclose or a refusal to answer a particular question

before Congress. Instead, this Indictment includes specific details regarding the "when, how, and

with whom" of the alleged fraud scheme, including the identification of specific false statements

in furtherance of the scheme. *See United States v. Rigas*, 490 F.3d 208, 229-30 (2d Cir. 2007)

("When the crime charged involves making false statements, the 'core of criminality' is not the

substance of the false statements but rather that knowing falsehoods were submitted . . . . [W]e

must read an indictment to include facts which are necessarily implied by the specific allegations

made"; finding indictment put defendants on notice of the "core criminality" the government

intended to prove at trial where it alleged that the defendants caused their company to "record false

and misleading entries in its books and records for the purpose of substantiating [the company's]

false and fraudulent loan compliance reports"); *United States v. Raniere,* 384 F. Supp. 3d 282,

308-09 (E.D.N.Y. 2019) (finding that an indictment alleging that the defendant "submitted

37

materially false and fraudulent statements" as part of the alleged fraud scheme did not need to

"identify those statements or explain why they were false" to ensure that the defendant had proper

notice of the charges against him).

    *ii.   <u>The Defendants' "As Applied" and "Novel" Vagueness Challenges
Also Fail</u>*

The defendants next argue that Section 1343 is unconstitutionally vague as applied to the

unique facts of this case because (i) it did not provide fair notice that the defendants' conduct was

unlawful and (ii) the wire fraud theory is "novel." (Dkt. 49 at 10-19).

As a threshold matter, the defendants' vagueness claim as to the applicability of the wire

fraud statute to their conduct, (Dkt. 49 at 10-11), is not properly brought at the motion to dismiss

stage. Vagueness challenges are "as applied" to the facts, so courts "must await conclusion of the

trial" to determine whether a statute is unconstitutionally vague in a particular case. *United States

v. Milani*, 739 F. Supp. 216, 218 (S.D.N.Y. 1990); *see also United States v. Rybicki*, 354 F.3d 124,

129 (2d Cir. 2003) ("Panel opinions of this Court have repeatedly held that when, as in the case

before us, the interpretation of a statute does not implicate First Amendment rights, it is assessed

for vagueness only 'as applied,' *i.e.*, in light of the specific facts of the case at hand and not with

regard to the statute's facial validity."); *Eisenberg,* 2023 WL 8720295, at *7 (denying defendant's

vagueness challenge as premature where the defendant similarly claimed that "all he did was

engage in open-market [cryptocurrency] trades that no one would understand to be unlawful";

noting that "the Court requires full factual development at trial before it can determine whether the

[statutes at issue] failed to provide Defendant fair warning that his conduct was prohibited by law,

as required by the Due Process Clause"). That is, in part, because "[o]bjections to vagueness under

the Due Process Clause rest on the lack of notice, and hence may be overcome in any specific case

where reasonable persons would know that their conduct is at risk." *Maynard v. Cartwright*, 486

U.S. 356, 361 (1988); *United States v. Nadi*, 996 F.2d 548, 550 (2d Cir. 1993) ("[O]ne whose conduct is clearly proscribed by the statute cannot successfully challenge it for vagueness.").[11]

These clear holdings put a quick end to the defendants' motion to dismiss on vagueness grounds. There is no basis to conclude from the Indictment that the defendants lacked notice that their actions were unlawful. Instead, the allegations clearly suggest that they "actually believed what they were doing was illegal." *United States v. Roberts*, 363 F.3d 118, 123 (2d Cir. 2004). *First*, the defendants took numerous steps to conceal their identity and participation in the fraud scheme by (i) establishing shell companies that were used as part of the fraud scheme and thereafter, to launder the fraud proceeds (Ind. ¶¶ 17-19, 31), (ii) researching ways to "wash crypto" to further conceal their identity (*id.* ¶ 19), and (iii) using a privacy layer network on the Ethereum

---

[11] The cases the defendants cite where courts dismissed charges based on vagueness challenges are easily distinguishable. (Dkt. 49 at 10-11 (citing *United States v. Matthews*, 787 F.2d 38 (2d Cir. 1986) and *United States v. Saathoff*, 708 F. Supp. 2d 1020 (S.D. Cal. 2010)). Unlike here, *Matthews* was a post-trial appeal from a criminal conviction under the securities laws. *Matthews*, 787 F.2d at 39. There, the Second Circuit reversed the defendant's conviction for failing to disclose criminal conduct in a proxy statement in violation of Section 14(a) of the Securities Exchange Act. *Id.* at 50. The Second Circuit noted that the evidence of the existence of a conspiracy to bribe tax officials was thin, reflected by the jury's acquittal on that count, and therefore, it was difficult to conclude that any "true" facts relevant to the count of conviction were actually omitted from the proxy statement. *Id.* at 45-46. This fact, along with failed attempts by the SEC to increase qualitative disclosures and prior case law reflecting the same, warranted the post-trial reversal. *See id.* at 47-48. None of these facts are applicable here. In *Saathoff*, city board members were charged with various honest services wire fraud violations for failing to disclose conflicts of interest. On a motion to dismiss, the district court observed that the right to honest services theory was one that had been identified as particularly problematic. 708 F. Supp. 2d at 126. In reaching its decision that the indictment was vague as applied to the defendants, the court also considered evidence derived from court hearings in the case over three years and parallel proceedings before the California Supreme Court in a case interpreting California's government employee conflict of interest statute that involved Saathoff, the defendant—*Lexin v. Superior Court of San Diego*, 47 Cal. 4th 1050 (2010). *Id.* at 1026-28, 1035. *Saathoff*—a 14-year-old, out-of-district case—presented a unique set of facts pertaining to a different criminal statute; did not address the "as applied" doctrine; reviewed historical proceedings that expanded beyond the indictment; and to-date, has only been cited by three out-of-district cases in either a negative or distinguishing manner.

blockchain, which enables users to conceal identity information, to establish the fraud scheme validators (*id.*). *Second*, in the months prior to the Exploit, Anton Peraire-Bueno ran "online searches related to Ethereum validator penalties for misconduct—a foreseen consequence of carrying out the Exploit." (*Id.*). Third, following the theft of the Victim Traders' money, the defendants took numerous steps over several months to off-ramp the fraud proceeds to traditional bank accounts "even though it was feasible, cheaper, and far simpler" to transfer the funds through other means. (*Id.* ¶¶ 30-31). Notably, the defendants took these actions *after* repeated requests from Victim-1, Victim-1's counsel, and a representative from Ethereum "to return the stolen funds," (*id.* ¶ 30), and *after* "foreign law enforcement froze approximately $3 million . . . of the fraud proceeds," (*id.* ¶ 31(b)). And finally—despite the defendants' claims that they "had no reason to know that their alleged conduct may be considered unlawful" (Dkt. 49 at 2)—during the time period in which the defendants were laundering the fraud proceeds, they searched online for, among other things, the very criminal statutes for which they were later indicted: "how long is us statue [sic] of limitations," "wire fraud statute/ wire fraud statue [*sic*] of limitations," "fraudulent Ethereum addresses database," "money laundering statue [*sic*] of limitations," "money laundering," "exploit," "computer fraud abuse act," and "does the united states extradite to [foreign country]." (Ind. ¶¶ 29, 32). These searches themselves expose the defendants' own actual awareness of the criminality of their conduct, even before their arrests on the charges contained in the Indictment.

   At best, the defendants' arguments do not challenge the legal sufficiency of the Indictment, but rather the potential strength of the Government's evidence. Those challenges, however, do not make the underlying statute as applied to their conduct any less clear. As the Supreme Court put it, "[c]lose cases can be imagined under virtually any statute. The problem that poses is

addressed, not by the doctrine of vagueness, but by the requirement of proof beyond a reasonable

doubt." *United States v. Williams*, 553 U.S. 285, 306 (2008). Likewise, the defendants' "novel

construction" argument, which they pursue through a lengthy recitation of their contested views

regarding the Ethereum Network; the existence (or non-existence) of protocols and norms

governing the MEV-Boost system; the nature of interactions between parties conducted through

smart contracts; and their attempt to villainize the Victim Traders to justify their own conduct

(Dkt. 49 at 10-19), is not a vagueness challenge. But rather, it is an attempt to litigate the substance

of whether they, in fact, intended to and did engage in a fraud scheme to steal the Victim Traders'

money. That is a jury argument, not an argument cognizable on a motion to dismiss.

Setting aside the premature timing of the defendants' vagueness challenge, their argument

that Counts One and Two should be dismissed as a "novel construction" as applied to the

defendants' conduct is also meritless. While a statute must give a defendant fair notice that his

conduct is unlawful, as the wire fraud statute here plainly does, there is no requirement that there

have been "a factual situation that is 'fundamentally similar'" to the crime charged. *Lanier*, 520

U.S. at 269; *Ponnapula v. Spitzer*, 297 F.3d 172, 183 (2d Cir. 2002) ("Due process is not, however,

violated simply because the issue is a matter of first impression."). The court in *United States v.*

Storm, 23 Cr. 430 (KPF), which involves the criminal prosecution of the creator and operator of a

particular cryptocurrency mixing service that executed anonymous, virtually untraceable

cryptocurrency transfers for customers, recently rejected nearly identical claims. (23 Cr. 430

(KPF), Dkt. 84 at 44-46 (Transcript of Proceedings as to Storm)). Like the defendants here, Storm

argued that the Indictment should be dismissed because "there [was] simply no precedent for the

expansive application of the statutes to his conduct," and that he had "found no judicial decisions"

prohibiting the alleged conduct. (*Id.* at 45). Judge Failla denied the defendant's "novel

construction" challenge, noting that "[d]ue process does not require the existence of an analogous

prior prosecution." (*Id.*).

Like this case, several of the cited precedents discussed above, including *Eisenberg* and

Storm, have raised some novel issues when they were brought. That is the inevitable result of the

application of longstanding criminal statutes to new technologies. Some case has to be the first.

United States v. Ulbricht, 31 F. Supp. 3d 540, 566 (S.D.N.Y. 2014) ("The fact that a particular

defendant is the first to be prosecuted for novel conduct under a pre-existing statutory scheme does

not ipso facto mean that the statute is ambiguous or vague or that he has been deprived of

constitutionally appropriate notice."); *United States v. Kinzler*, 55 F.3d 70, 74 (2d Cir. 1995)

("[C]laimed novelty of this prosecution does not help [defendant's] cause, for it is immaterial that

there is no litigated fact pattern precisely in point."). The defendants' criminal conduct may not

be identical in every respect to similar prior criminal schemes. That, however, does not constitute

a due process violation.

This case, in short, is one for the jury. The defendants violated well-established legal

principles prohibiting fraud. Their arguments to the contrary are fundamentally fact disputes for

trial, not for a motion to dismiss.[12]

II.   The Motion To Suppress Should Be Denied

The defendants move to suppress evidence seized in this case pursuant to an electronic

search warrant (the "Google Warrant") for the content contained in six Google LLC accounts (the

---

[12] The defendants also move to dismiss Count Three (conspiracy to commit money laundering), based entirely on their claim that Counts One and Two are defective. (Dkt. 49 at 33). For the reasons set forth above, the Indictment properly alleges wire fraud and a conspiracy to commit wire fraud. Because the defendants' motion to dismiss those counts is without merit, the defendants' motion to dismiss Count Three also fails.

"Google Accounts") belonging to the defendants on the grounds that the affiant "deliberately made false statements or recklessly disregarded the truth," invoking *Franks v. Delaware*, 438 U.S. 154 (1978). (*See* Dkt. 53). These accusations, and the motion itself, are entirely unfounded. The defendants' motion should be denied, without any need for a *Franks* hearing.

The defendants contend that the Google affidavit (the "Google Affidavit") "falsely asserted" the following six points outlined below:

1. The defendants baited their victims by proposing transactions that they had "no intention of executing" (Dkt. 53 at 5-8);

2. The defendants targeted "more obscure cryptocurrency tokens" (*id.* at 8-9);

3. The Victim Traders specialized in "cryptocurrency arbitrage" (*id.* at 9-10);

4. The defendants "altered" transactions (*id.* at 11-12);

5. The Google Affidavit manipulated a diagram in a manner that "undermines" the fraud allegations (*id.* at 12-14); and

6. The defendants "tampered" with the blockchain itself (*id.* at 14-16).

The defendants motion fails to set forth any constitutional violation because these purported "falsehoods" cited by the defense are in fact accurate statements, especially when viewed in the context of the full affidavit, and regardless, they are plainly immaterial to the probable cause determination. Certainly, none of these statements evidence an effort to intentionally mislead the Magistrate Judge who authorized the Warrant. In sum, the defendants' suppression argument depends on asking this Court to ignore the totality of evidence set forth in a 48-page warrant in favor of a self-serving characterizations of a handful of discrete facts. The Court should reject that invitation. Because the challenged search and seizure was supported by probable cause and executed pursuant to a lawful Warrant issued by a Magistrate Judge, and

accordingly law enforcement agents relied upon the Warrant in good faith to execute the search of the Google Accounts, the defendants' motion should be denied in its entirety.

A. Relevant Background[13]

This case arises from a months-long investigation conducted by the Internal Revenue Service-Criminal Investigation ("IRS-CI"), which was prompted by public reports in April 2023 that certain individual(s) had executed a multi-step computer exploit that targeted specific cryptocurrency trades on a decentralized exchange in the time period between the initial trade request and publication of the trades on the blockchain.

To provide context for the Magistrate Judge regarding the alleged crimes, the Google Affidavit provided background concerning cryptocurrency and cryptocurrency infrastructure relevant to the investigation. (Dkt. 56-8 ¶¶ 13-15). The Google Affidavit thereafter included a summary of information provided by Victim-1 and a representative of a company that designed the MEV-Boost system (the "MEV-Boost Representative"), which described in detail the (i) trading patterns of MEV Bots operated by Victim-1, including how Victim-1's trades were typically processed using the MEV-Boost system; and (ii) the process by which the defendants obtained Victim-1 and other Victim Traders' money, including the use of the Lure Transactions

---

[13] As explained below, a hearing is not required to deny the defendants' motion. The facts recited herein rely on the defendants' declaration and supporting papers. For the reasons outlined in footnote 15, all citations herein are to the Google Warrant and Affidavit, Docket Number 56-8. Where applicable, citations refer to paragraph numbers contained therein. Where paragraph numbers are inapplicable, citations in Section II refer to the ECF-filed page number to differentiate between the Google Warrant and Affidavit, which are combined as one document in Docket Number 56-8.

(referred to in the Google Affidavit as "Honeypot Transactions"),[14] the Malicious Validator, and the False Signature. (*Id.* ¶¶ 16, 18).

The Google Affidavit included additional corroboration of the information obtained from Victim-1 and the MEV-Boost Representative. This evidence not only corroborated the description of the Exploit as summarized by the witnesses and public information, but also described extensive efforts by the defendants to conceal their identities both prior to and after the Exploit. This evidence, among other things, included: (i) a publicly available screenshot of the computer code from the Corrupt Block containing the False Signature, (Dkt. 56-8 ¶ 18(d)); (ii) extensive cryptocurrency tracing analyses linking the defendants to the creation of the Exploit Validators; the use of numerous privately held cryptocurrency addresses, virtual private networks ("VPN"), foreign cryptocurrency exchanges, and a privacy layer protocol, as well as the receipt of the fraud proceeds—all of which was graphically outlined in an appendix (*id.* ¶¶ 20-31, and Appendix 1); (iii) financial records (*id.* ¶¶ 22, 25); (iv) business incorporation records (*id.* ¶¶ 26-28); (v) Internet protocol ("IP") address analyses linking the defendants to the Exploit (*id.* ¶¶ 29-31); and (vi) blockchain data showing that the Malicious Validator was penalized for failing to act in accordance with validation protocols (*id.* ¶ 18(g), 21(c)).

Magistrate Judge James L. Cott authorized the Google Warrant on January 5, 2024. (Dkt. 56-8 at 50).[15]

---

[14] The Google Affidavit references to "Honeypot Transactions" and "Lure Transactions" are equivalent to the Indictment's references to the "Lure Transactions" and "Bait Transactions," respectively. For consistency between the Indictment and the Google Affidavit, and to minimize any risk of confusion, this opposition refers to the "Honeypot Transactions" and the "Lure Transactions" in the Google Affidavit as the "Lure Transactions" and the "Bait Transactions," respectively.

[15] On January 30, 2024, Magistrate Judge Cott signed a second Google Warrant (the "Second

B. Applicable Law

A warrant issued by a neutral and detached magistrate carries a presumption of validity. *United States v. Rosa*, 11 F.3d 315, 326 (2d Cir. 1993) (warrant issued by a neutral and detached magistrate is "entitled to substantial deference, and doubts should be resolved in favor of upholding the warrant"); *see also United States v. Travisano*, 724 F.2d 341, 345 (2d Cir. 1983) (magistrate judge's "finding of probable cause is itself a substantial factor tending to uphold the validity of [the] warrant"). Thus, where a defendant specifically argues that an affidavit in support of a search warrant contained deliberately misleading or recklessly false information, "a defendant must make a substantial preliminary showing that: (1) the claimed inaccuracies or omissions are the result of the affiant's deliberate falsehood or reckless disregard for the truth; and (2) the alleged falsehoods or omissions were necessary to the judge's probable cause finding." *Salameh*, 152 F.3d at 113 (citation and internal quotation marks omitted); *see also United States v. Awadallah*, 349 F.3d 42, 64 (2d Cir. 2003) (noting that "in order to invoke the *Franks* doctrine, [a defendant] must show that there were intentional and material misrepresentations or omissions in [the] warrant affidavit"). As the Supreme Court explained in *Franks*:

> to mandate an evidentiary hearing, the challenger's attack must be more than
> conclusory and must be supported by more than a mere desire to cross-examine.
> There must be allegations of deliberate falsehood or of reckless disregard for the
> truth, and those allegations must be accompanied by an offer of proof. They should

Google Warrant"). (Dkt. 56-9 at 16). As outlined in the affidavit in support of the Second Google Warrant (the "Second Google Affidavit"), the Google Warrant "inadvertently omitted a request directing the Provider to provide . . . 'Web & App Activity, Search, Chrome, and Browsing History' . . .[and] 'Google Services Data[.]'" (*Id.* ¶ 9). In its request for this information, the Second Google Affidavit clarified that "the instant warrant requests this information based on the probable cause outlined in the [Google Warrant and Affidavit, attached thereto as Exhibit 1]. No other modifications to the [Google Warrant and Affidavit] have been made." (*Id.* ¶ 10). Because there are no differences between the Google Warrant and Affidavit and Second Google Warrant and Second Google Affidavit relevant to the defendants' suppression motion, all citations herein are to the Google Warrant and Affidavit, Docket Number 56-8.

point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons. Affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained. Allegations of negligence or innocent mistake are insufficient.

Franks v. Delaware, 438 U.S. 154, 171 (1978).

A defendant seeking to make the first required showing of an intentional or reckless misstatement or omission must show more than inadvertent error. "[E]very statement in a warrant affidavit does not have to be true," *United States v. Martin*, 426 F.3d 68, 73 (2d Cir. 2005), and "the mere intent to exclude information is insufficient . . . An affiant cannot be expected to include in an affidavit every piece of information gathered in the course of an investigation." *Awadallah*, 349 F.3d at 67-68 (citation omitted). As the Second Circuit recently explained:

A [warrant] applicant does not *necessarily* act with 'reckless disregard for the truth' simply because he or she omits certain evidence that a reviewing court, in its judgment, considers to be 'clearly critical.' Rather, the reviewing court must be presented with credible and probative evidence that the omission of information in a wiretap application was 'designed to mislead' or was 'made in reckless disregard of whether it would mislead.'

Rajaratnam, 719 F.3d at 153-54 (emphasis in original) (quoting *Awadallah*, 349 F.3d at 64). "To prove reckless disregard for the truth," a defendant must "prove that the affiant in fact entertained serious doubts as to the truth of his allegations." *Id.* (quoting *United States v. Whitley*, 249 F.3d 614, 621 (7th Cir. 2001)).

The moving defendant must also prove that any misstatements or omissions alleged were material. To determine if the false information was material, *i.e.*, "necessary to the issuing judge's probable cause determination, . . . a court should disregard the allegedly false statements and determine whether the remaining portions of the affidavit would support probable cause to issue the warrant." *United States v. Canfield*, 212 F.3d 713, 718 (2d Cir. 2000) (citing *Salameh*, 152 F.3d at 113). "If the corrected affidavit supports probable cause, the inaccuracies were not material

to the probable cause determination and suppression is inappropriate. As with the inclusion of false information, 'omissions from an affidavit that are claimed to be material are governed by the same rules.'" *Id.* (quoting *United States v. Ferguson*, 758 F.2d 843, 848 (2d Cir. 1985)); *see also Rajaratnam,* 719 F.3d at 146 (stating that, to determine whether omissions are material, a court should consider whether, "if the omitted material had been included in the affidavit, the affidavit would still establish probable cause" (citation omitted)).

The movant bears a "heavy burden" when challenging a warrant for lack of probable cause. *Rivera v. United States*, 928 F.2d 592, 602 (2d Cir. 1991). When reviewing the legality of previously issued search warrants, reviewing courts "accord 'great deference' to a judge's determination that probable cause exists, and . . . resolve any doubt about the existence of probable cause in favor of upholding the warrant." *United States v. Salameh*, 152 F.3d 88, 112 (2d Cir. 1998) (quoting *United States v. Jakobetz*, 955 F.2d 786, 803 (2d Cir. 1992)). The reviewing court's duty is "simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). "Courts must refrain from invalidating judicially authorized warrants based on 'hypertechnical' interpretations of affidavits." *United States v. Williams*, 13 Cr. 419 (DLI), 2016 WL 4257346, at *3 (E.D.N.Y. Aug. 11, 2016) (quoting *United States v. Ventresca*, 380, U.S. 102, 107 (1965)).

In assessing a defendant's claims, courts recognize that "probable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." *Gates*, 462 U.S. at 232. When making a probable cause determination, "[t]he task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there

48

is a fair probability that contraband or evidence of a crime will be found in a particular place." *Id.*

at 238. Probable cause requires the establishment of "only the probability, and not a prima facie

showing, of criminal activity." *Id.* at 235.

C. Discussion

1. There Is No Basis for a *Franks* Hearing Because the Google Affidavit Is Accurate

None of the six purported "deliberate falsehoods" outlined in the defendants' motion comes

close to justifying suppression. In fact, as discussed below, the 48-page Google Affidavit is

accurate.   And to the extent there were any arguable affirmative inaccuracies or omissions, the

defendants have failed to show that they are material, let alone that the affiant acted with the intent

to mislead or in reckless disregard for the truth. Moreover, the probable cause supporting the

Google Warrant did not rest any of these isolated statements. As the Google Warrant and the later

Indictment make plain, the defendants engineered an elaborate and sophisticated scheme to

brazenly steal millions of dollars through fraud. The defendants' critiques of the Google Affidavit

and examination of specific phrases in isolation fail to undermine that fundamental premise.

Accord District of Columbia v. Wesby, 583 U.S. 48, 60-61 (2018) (explaining that because the

"whole is often greater than the sum of its parts—especially when the parts are viewed in

isolation," the probable cause determination is a "totality of the circumstances" analysis that

"precludes [a] sort of divide-and-conquer analysis"). As such, the defendants have failed to meet

the stringent standard for a *Franks* hearing or suppression under *Franks*. Each of the defendants'

purported "deliberate falsehoods" is addressed below.

i. The Trade Requests

The defendants contend that the Google Affidavit "falsely claimed that the [defendants]

'sent requests for trades that *they had no intention of executing* (*e.g.,* [the Lure Transactions])."

(Dkt. 53 at 5 (emphasis in original) (citing Dkt. 56-8 ¶ 19)). This argument is meritless, as defendants fail to show that such a statement was false in the context of the fraud scheme described in the affidavit, much less material to the magistrate judge's probable cause determination.

The defendants' claim rests on an overly literal focus on the phrase "no intention"—essentially claiming that because the Lure Transactions were ultimately published to the blockchain *after* the alleged crime was complete, the defendants must have had an "intention" to execute them.[16] This strained interpretation of the affidavit is fundamentally flawed. The Lure Transactions, as supported by the witness statements and corroborating facts, were not *bona fide* trades. Notably, the reference to the defendants' "intention" with respect to the Lure Transactions followed a detailed description of the Exploit, including facts that Lure Transactions were designed to (and did) create a false appearance of a profitable trading opportunity, which caused the Victim Traders to part with their money in a manner essential to the theft. (*See* Dkt. 56-8 ¶¶ 16(c) (describing bundled trade requests and the effect of an "attractive mempool trade"), 16(i) (describing bait transactions), 17(b)-(d), (f) (describing the purpose of the Lure Transactions, Tampered Transactions, and Malicious Validator), 18(e) (same)). As the Google Affidavit outlined, the Lure Transactions were submitted to the mempool to ensure the Victim Traders included them in proposed bundles that, based on the scheme, would be (and were) replaced within

---

[16] The defendants point out, and the Government agrees, that the Lure Transactions were published to the blockchain *after* the alleged crime was complete. (*See* Dkt. 53 at 8 ("the [public] record of the [Lure Transaction] shows it, too, was a 'success' and included only two blocks *later*" (emphasis added)).

milliseconds with the Tampered Transactions using the False Signature and Malicious Validator in order to steal the Victim Traders' money. (*Id.* ¶¶ 17(b)-(d), (f), 18(e)).

The fact that the Lure Transactions were ultimately published to the blockchain after the crime was complete does not, in any way, negate the probable cause inference, supported by ample facts in the Google Affidavit, that the defendants had a deceptive intent at the time of submitting the Lure Transactions to the mempool. (*See* Dkt. 56-8 ¶¶ 16(i), 17(b) 17(d)-(h), 18(e)-(g) (describing the fraud scheme generally, including the purpose of the Lure Transactions, in coordination with the False Signature, Malicious Validator, and Tampered Transactions), 22-31 (outlining actions of concealment further indicative of fraudulent intent)). *See Gates*, 462 U.S. at 230, 232 (observing that "probable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts," and endorsing a "totality-of-the-circumstances approach" to probable cause); *United States v. Falso,* 544 F.3d 110, 117 (2d Cir. 2008) (same); *Rivera*, 928 F.2d at 602 ("Where the circumstances are detailed, where reason for crediting the source of information is given, and when a magistrate has found probable cause, the courts should not invalidate the warrant by interpreting the affidavit in a hypertechnical, rather than a commonsense, manner[.]").

Essentially, the defendants argue that the Google Affidavit was false based on their view that relying on circumstantial evidence in support of the agent's description of the intent for submitting the Lure Transactions was improper. (Dkt. 53 at 5). But the defense's subjective view does not show in any way that the statement in the Google Affidavit was demonstrably *false*, let alone knowingly, intentionally, or even recklessly so. Simply put, the defendants' contention that their *post hoc* interpretation of a single phrase in the affidavit establishes the *falsity* of the phrase or the bad faith of the affiant is entirely without basis, ignores the support for the accuracy of that

51

phrase when reading the affidavit as a whole, and fails to meet the *Franks* standard required to trigger a challenge to the validity of the Google Warrant.[17]

> ii. *"More Obscure Tokens"*

Next, the defendants argue that the agent "deliberately misled the court" to believe that the defendants were "operating in some small, dark corner of the cryptocurrency world" by describing the Lure Transactions in the Google Affidavit as including "more obscure cryptocurrency tokens." (Dkt. 53 at 8-9 (citing Dkt. 56-8 ¶ 17(b))). The basis for this contention is that Aave and Shiba Inu tokens, which were included in the Lure Transactions, are—according to the defendants—actively traded tokens. (*Id.*) This amounts to quibbling over the connotation of descriptive language ("more obscure") as opposed to any concrete inaccuracy. As discussed below, the statement is entirely accurate in context and the description is immaterial to the Google Affidavit as a whole. The contention that Agent Dias "deliberately misled" the Magistrate Judge, (Dkt. 53 at 9), by calling some tokens "more obscure" than others borders on the frivolous.

As a threshold matter, the defendants mischaracterize the Google Affidavit. The single reference to "more obscure cryptocurrency tokens" was in the context of describing how the Lure Transactions were able to successfully cause the Victim Traders to propose bundles that included them. In particular, the Google Affidavit explained that the Lure Transactions included "trade requests with high slippage parameters for more obscure cryptocurrency tokens, such as Stargate

---

[17] Contrary to the defendants' assertion, (Dkt. 53 at 5-8), the Google Affidavit never stated or implied that the Tampered Transactions were not executed to the blockchain—so there was no false statement in the Google Affidavit on this score. Indeed, the Google Affidavit made clear that the execution of the Tampered Transactions to the blockchain was essential to the scheme. In fact, that was the entire point. (Dkt. 56-8 ¶¶ 17(d)-(e), (g), 18(e)).

Token ("STG"), Aave Token ("AAVE"), Shiba Inu ("SHIB"), and Curve DAO Token ("CVR"), *that have smaller liquidity pools*." (Dkt. 56-8 ¶ 17(b) (emphasis added)).

Notably, the defendants' argument makes no reference to the size of the Lure Transactions' liquidity pools at the time of the Exploit—one of the variables identified in the Google Affidavit as relevant to the operational success of the Lure Transactions (and a variable the defendants all but concede they were targeting as part of the Exploit). (*See* Dkt. 53 at 9 (noting that the victims engaged in trading "within individual liquidity pools")).   The Google Affidavit provided background information about decentralized exchanges, liquidity pools, and why smaller liquidity pools typically present better cryptocurrency arbitrage trading opportunities. (Dkt. 56-8 ¶¶ 13(f), (h), 17(b)). The phrase "more obscure tokens" was not inaccurate, specified the tokens at issue, and explained their comparative obscurity—in contrast to more well-known coins such as Bitcoin or Ether—as relating to their "smaller liquidity pools." There is simply no credible argument that omitting the single reference to "more obscure" tokens from the Google Affidavit was material to the Government's showing of probable cause in light of the other uncontested facts included in the warrant: indeed, if "more obscure" were omitted, the affidavit would read "[o]n or about the day of the Exploit, the hacker(s) deployed [the Lure Transactions] that included trade requests with high slippage parameters for ~~more obscure~~ cryptocurrency tokens, ...that have smaller liquidity pools." (*See* Dkt. 56-8 ¶ 17(b)).

iii. *"Sandwich Attackers"*

The defendants argue that the agent "falsely claimed, 'the [alleged] Exploit targeted particular victims that specialize in high-frequency *cryptocurrency arbitrage trading*, which is designed to take advantage of *price differences* between identical or similar assets in *different markets*." (Dkt. 53 at 9 (emphasis and alterations in the original)). According to the defendants,

this is false and misleading because the Victim Traders do not engage in arbitrage trading in "different markets," but rather engage in trading designed to "manipulate prices within individual liquidity pools." (*Id.* at 9-10). The defendants contend that these types of trades are correctly identified as "sandwich attacks." (*Id.* at 9).

The defendants once again quibble over word choice, focusing on a hyper-technical interpretation of a few words to the exclusion of the full affidavit. Not only is this contrary to the facts of the Google Affidavit, but contrary to governing law when reviewing for probable cause. To the extent that there was any arguable error in the Google Affidavit by the single reference to "*different markets*" as opposed to "*individual liquidity pools*," such a hyper-technical error certainly cannot be characterized as material because here, the Google Affidavit further described the Victim Traders' trading strategy in detail *and* in a manner that comports with the defendants' preferred description—even referencing the defendants' preferred terminology ("sandwich trades," "sandwich attacks," "sandwich bundles")—all facts that the defendants readily concede, as they must. (*See* Dkt. 53 at 9 (citing Dkt. 56-8 ¶¶ 17(b), 17(h), and 12 ("Dias describes the recipe for a 'sandwich attack' in similar terms," and citing Dkt. 56-8 ¶¶ 16(c)(i)-(iii))). The Google Affidavit made no effort to conceal this characterization. In fact, the affidavit referred to this type of trading activity as "sandwich trades" on five separate occasions. (*Id.* ¶¶ 16(c)(ii), 17(b), 17(d), 17(h) 23(a)). In short, the information that the defendants claim was falsely omitted was in fact contained elsewhere in the same Google Affidavit. This is further proof that the defendants cannot show any intentional effort to mislead the judge.

At base, the defendants' real contention is not that the Google Affidavit was inaccurate or misleading, but that it failed to set forth their anticipated defense—namely, that because the victims were (according to the defendants' self-serving and contested characterizations) engaged

54

in "market manipulation," the defendants did nothing wrong when they took steps to steal the victims' money.[18] Even assuming there is any merit to the defendants' self-serving, *ex post* justification concerning the legality of their actions (which the Government disputes both factually and legally), such an argument is immaterial to the probable cause determination. *See, e.g.*, *United States v. Fama*, 758 F.2d 834, 838 (2d Cir. 1985) ("The fact that an innocent explanation may be consistent with the facts alleged, however, does not negate probable cause. Neither should it preclude a good faith belief in probable cause"). Here, the facts alleged in the Google Affidavit through the Victim-1 and MEV-Boost Representative summaries and corroborating evidence, including the countless ways the defendants concealed their identities, evidence that foreign law enforcement had frozen a portion of the fraud proceeds, and records that other Ethereum users penalized the defendants for their actions pertaining to the Exploit, (Dkt. 56-8 ¶¶ 16-31), more than established a "probability" of criminal activity. *Gates*, 462 U.S. at 235 (noting that probable cause requires the establishment of "only the probability, and not a prima facie showing, of criminal activity").

Moreover, as outlined also in Section III, it also bears noting that such an argument is also irrelevant to the jury's ultimate determination of guilt, which focuses on the defendants' *mens rea*. *See United States v. Connolly*, 16 Cr. 370 (CM), 2019 WL 2125044, at *13 (S.D.N.Y. May 2,

---

[18] The defendants' assert that "sandwich" trading is a form of "market manipulation" based on citations to a handful of Internet posts in their motion to compel, (Dkt. 50 at 9-10), which notably appear to have been published after the Exploit and even after the Google Warrant, or simply do not contain a publication date at all. The issue is that this assertion is nothing more than another improper attempt to litigate the sufficiency of evidence, as opposed to the sufficiency of the Indictment, or here, the Google Affidavit. To the extent that any of these arguments are relevant to the defendants' *mens rea* at the time of the Exploit (as they contend), they are more appropriate for *Daubert* motions and motions *in limine*, where cited sources and any arguments derived from them can be appropriately analyzed for reliability and relevance.

2019) ("'[E]verybody is doing it' is not a defense to the crime of wire fraud or conspiracy to commit wire fraud; just as 'everybody speeds' is not a defense if your car happens to get picked up on the radar."); *United States v. Korogodsky*, 4 F. Supp. 2d 262, 265 (S.D.N.Y. 1998) ("It is no defense that the victims of the fraud may have been engaged in some misconduct."); *see also United States v. Oldbear*, 568 F.3d 814, 821 (10th Cir. 2009) (holding that "only [defendant's] actions and state of mind were material to her guilt," and "the fact that others may have been the beneficiaries of improper conduct does nothing to excuse [the defendant].").

iv.   "*Altered Transactions*"

The defendants contend that the agent "misled" the Court by "incorrectly" alleging that the defendants "deliberately altered certain transactions," where in practice, the defendants, in their view, only "chang[ed] the *order* of potential transactions" and not the "terms of any requested transactions." (Dkt. 53 at 11). The defendants' contention is that the use of the word "alter" instead of "re-order" was an intentional lie to the Magistrate Judge. This argument is far afield from either fact or law. At most, the defendants point to a word-choice disagreement. Webster's Dictionary defines "alter" as "to make different without changing into something else." (*See* https://www.merriam-webster.com/dictionary/alter, last accessed January 8, 2024). The Google Affidavit makes clear, in accordance with this definition, that the term "altered" refers to the replacement of the Lure Transactions with the Tampered Transactions, which were published on the Corrupt Block, along with the Victim Traders' frontrun and backrun trades. (Dkt. 56-8 ¶¶ 14(c)(i), 17(b), (d)-(e), 18(g) ("[T]he Malicious Validator replaced approximately eight [Lure Transactions]" with the "inverse trades (the 'Tampered Transactions').")). The only reference to changing the "terms of any requested transaction" comes from the defendants' own motion.

56

Simply put, the Google Affidavit is accurate.[19]

v. The MEV Boost Diagram

The defendants contend that a diagram referenced in the Google Affidavit, "omit[ted]
critical information that undermines the fraud allegations." (Dkt. 53 at 12-13). The diagram at
issue is referenced below and cited in the Google Affidavit in paragraph 6:
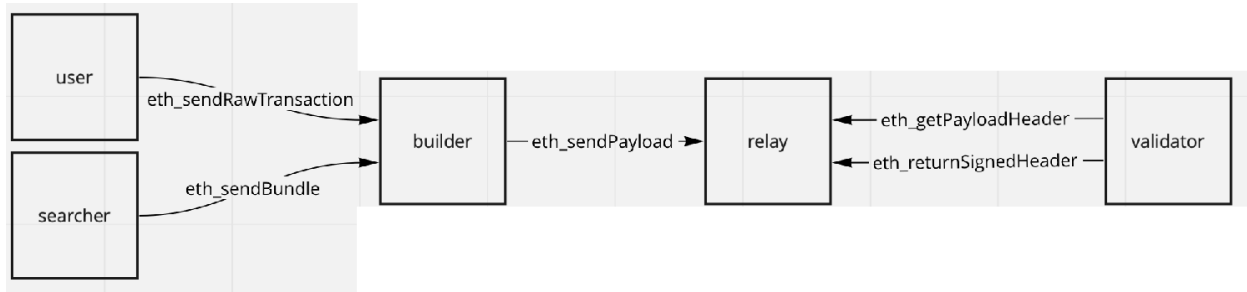
The diagram preceded a paragraph generally describing the interaction among third parties
using the MEV-Boost system in the block proposal process. (Dkt. 56-8 ¶ 15(c)(1)-(5)). After
outlining the roles of a user, searcher, builder, validator, and a relay, the Google Affidavit included
the diagram referenced above and described it as "a diagram of the varying participants in the
mempool and *general* sequence of events, moving left to right, involved in executing a
cryptocurrency transaction on a [decentralized exchange] using the MEV-Boost system[.]" (*Id.*

---

[19] In what appears to be a vigilante defense, the defendants also contend that "altered" is inaccurate
because the scheme as charged was simply "frustrat[ing] the efforts by three sandwich attackers
to prey on retail users of the Ethereum network." (Dkt. 53 at 12). This argument misreads the
Google Affidavit and Indictment and merely reasserts defendants' anticipated trial defense that
their actions were justified in light of the victims' actions. As previously described, such an
argument is irrelevant to a probable cause determination, legally and factually meritless, and in
any event, more appropriately litigated through *Daubert* motions and motions *in limine*.

¶ 15(c)(6) (emphasis added)). The Google Affidavit did not assert that the diagram included all technical details concerning the interactions among the third parties depicted.

According to the defendants, the purported critical omission from the diagram above is that it "cropped" out a reference to a purported "escrow" party that, notably, was *never* adopted by the MEV-Boost system. (Dkt. 53 at 13 (describing the omitted reference to an "escrow," but conceding that "the MEV-Boost system did not adopt that design")). This argument is totally nonsensical. Based on the defendants' own admission—that there was not an "escrow" party in the MEV-Boost system—inclusion of the very information they claim should have been included would have rendered the diagram *inaccurate*. *See Rajaratnam,* 719 F.3d at 146-47 (in the context of omissions, courts "insert the omitted truths" into the hypothetical corrected affidavit to determine if probable cause exists). Put differently, and highlighting the absurdity of the defendants' argument, inclusion of an independent "escrow" entity in the diagram would actually have described a version of the MEV Boost infrastructure that was *never* adopted in practice, and thus, *never* described anywhere in the Google Affidavit.

Finally, the defendants are flat wrong that the Google Affidavit (absent the depiction of an escrow entity that was never adopted) "erroneously suggests that the relay does not provide any information to the validator." (Dkt. 53 at 12; *see also id.* at 13 ("By cropping the escrow from his altered diagram and failing to explain the context of the original image, Dias hid from the court the undisputed fact that the validator appropriately receives information from the relay.")). On the contrary, the Google Affidavit explained on more than one occasion that as a standard part of the validation process, the relay sends information to the validator:

> ▪ The relay then submits the blockheader [to the validator], which as described above, lists the potential rewards a validator may receive, but does not contain a list of the transactions contained in the proposed block. The validator

communicates with the relay to get the most profitable blockheader, which it attests to by signing with its public key.   After confirming through its signature that it will validate the contents of the block as proposed, the relay releases the **execution payload** (*i.e.*, the message containing the list of transaction to be added to the block) to the validator for validation and block publication.   (Dkt. 56-8 ¶ 15(c)(5) (notably, the paragraph immediately preceding the contested diagram)).

▪ The relay requests a validator's confirmation signature by sending, in the first instance, a blockheader to a validator, which contains basic information about the proposed block, including the proposed block's expected MEV. (Dkt. 56-8 ¶ 18(b)).

Thus, far from omitting "critical information that undermines the fraud allegations," the Google Affidavit, including its narrative text and corresponding illustrative diagrams, accurately describes the MEV-Boost system and the interaction amongst third parties using that system.

Most importantly, the defendants fail to show how any of their points were material to establishing probable cause. For this reason alone, the defendants' motion to suppress on this basis fails on its face.

vi. "*Tampered With The Blockchain*"

Last, the defendants argue that the agent "misled the Court when he falsely suggested the Peraire-Buenos somehow 'tamper[ed]' with the 'transparent and previously believed tamper-proof ledger system.'" (Dkt. 53 at 14). This argument is meritless, as they once again fail to show it is false, but rather based on their contested view of the facts, and further, fail to show it is material to the probable cause determination.

The Google Affidavit made clear that the Exploit targeted the process and protocols by which transactions are validated and added to the blockchain—not the post-publication of trades. (Dkt. 56-8 ¶¶ 8 (describing the Exploit as targeting cryptocurrency trades "in the period of time between the initial trade request and publication of the trade on the blockchain"); *see also* ¶ 14(a),

(c), 16(f), (g), 17(d), 18(a), (e) (same)). However, in much the same way that an infection targets and weakens an immune system, the Google Affidavit accurately described the Exploit as a scheme designed to "exploit the infrastructure of the blockchain"—namely, its block-building process and protocols. (Dkt. 56-8 ¶ 8 (emphasis added)). Simply put, the defendants' contested view concerning the impact of their own alleged conduct does not make the statement inaccurate or misleading—let alone, intentionally false—when viewed in the context of the scheme's details set forth fully in the affidavit. *See Fama*, 758 F.2d at 838 ("The fact that an innocent explanation may be consistent with the facts alleged, however, does not negate probable cause. Neither should it preclude a good faith belief in probable cause")

In sum, when stripped from hyperbole and placed in context of "all the circumstances set forth in the affidavit," *Gates*, 462 U.S. at 238, the defendants fail to establish that any of their purported "deliberate falsehoods" are, in fact, inaccurate or misleading, never mind material to probable cause. Nor have the defendants made a threshold showing that any of the alleged misstatements or omissions were made with the intent to mislead or in reckless disregard for the truth. Simply stating as much in conclusory fashion, does not make it so. An "affiant cannot be expected to include in an affidavit every piece of information gathered in the course of an investigation," *Awadallah,* 349 F.3d at 67-68, especially in a case like this where the defendants' conduct involved an intricate series of highly technical and highly synchronized steps to not only commit the crimes, but conceal their identities. Even a failure to summarize every piece of information or cite every statement with perfect precision does not amount to reckless disregard for the truth. *See, e.g.*, *Martin*, 426 F.3d at 73; *Awadallah*, 349 F.3d at 64; *Lahey,* 967 F. Supp. 2d at 708 ("All storytelling involves an element of selectivity.").

Here, the defendants have failed to demonstrate that the "affiant in fact entertained serious doubts as to the truth of his allegations." *Rajaratnam*, 719 F.3d at 154. The fact that the defendants are even contending to this Court that these arguments are a basis for finding that a federal agent intentionally deceived a federal magistrate judge is deeply troubling. *Cf. Falso*, 544 F.3d at 125 (noting that a "presumption of validity attaches to a law enforcement affidavit"). Accepting the defendants' arguments based on, at most, their own contested views of discrete facts and preferred characterizations in lieu of the totality of the circumstances set forth in the Google Affidavit is not the law and would enable defendants to fatally undermine any properly conducted investigation with the benefit of hindsight and based on their own subjective disagreement with the facts. Instead, the *Franks* standard is rightly a "high one," *Rivera,* 928 F.2d at 604, and one the defendants have plainly failed to meet here.

2. Even if the Google Affidavit Contained Inadvertent Errors, the Evidence Nevertheless Should Not Be Suppressed Under the Good Faith Exception

While the Affidavit set forth an abundant basis for a finding of probable cause to seize and search the Google Accounts, were the Court to find that the Affidavit is somehow lacking, suppression nevertheless would be unwarranted under the good faith exception.

The good faith exception provides that "evidence obtained by officers in objectively reasonable reliance on a warrant subsequently invalidated by a reviewing court is not generally subject to exclusion." *United States v. Raymonda*, 780 F.3d 105, 118 (2d Cir. 2015) (citation and internal quotation marks omitted). This is because "[w]hen an officer genuinely believes that he has obtained a valid warrant from a magistrate and executes that warrant in good faith, there is no conscious violation of the Fourth Amendment, and thus nothing to deter." *Id.* (citing *United States*

v. Leon, 468 U.S. 897, 920-21 (1984)) (internal quotation marks omitted). Indeed, as the Supreme

Court has explained:

> Exclusion exacts a heavy toll on both the judicial system and society at large. It almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence. And its bottom-line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment. Our cases hold that society must swallow this bitter pill when necessary, but only as a last resort. For exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs.

Davis v. United States, 564 U.S. 229, 237 (2011) (citations and internal quotation marks omitted).

The good faith exception applies where the officer's reliance on the duly issued warrant is

"objectively reasonable." *Id.* Thus, the good faith exception does not apply in four circumstances:

"(1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate

wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of

probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially

deficient that reliance upon it is unreasonable." *Raymonda*, 780 F.3d at 118.

Here, law enforcement acted in reasonable reliance on a valid warrant issued by a

magistrate judge. As outlined above, there is no showing that law enforcement knowingly misled

the court. The Google Affidavit, which contains 48 pages of factual allegations and summaries of

evidence, certainly was not "so lacking in indicia of probable cause as to render reliance upon it

unreasonable," nor was the warrant "so facially deficient that reliance [was] unreasonable."

Raymonda, 780 F.3d at 118 (citing *Clark*, 638 F.3d at 100). And there is no evidence, nor any

allegation, that Magistrate Judge Cott "wholly abandoned . . . [his] judicial role." *Id.*

In sum, the Google Affidavit was sufficient to establish probable cause, and the Google

Warrant was lawfully issued. Even if the Google Affidavit fell short (which it did not), the fruits

62

of the search should not be suppressed because the agents acted in good faith reliance on the

Google Warrant.

III.   The Motion for Immediate Production of Purported *Brady* Material Should Be Denied

The defendants seek an order directing the Government to search for and produce three

categories of evidence that they claim are exculpatory: (i) material tending to show that the Victim

Traders were engaged in trading strategies known as "sandwich attacks"; (ii) materials tending to

show that "sandwich attacks" are a form of market manipulation; and (iii) information regarding

the anonymity of the Victim Traders (the "Categories"). (Dkt. 51 at 4-14). The defendant's motion

must be denied for several reasons.

As a threshold matter, "it is well established that the Government's 'discovery and

disclosure obligations extend *only* to information and documents in the government's

possession.'" *United States v. Avenatti*, 559 F. Supp. 3d 274, 280 (S.D.N.Y. 2021) (quoting *United

States v. Brennerman*, 818 F. App'x 25, 29 (2d Cir. 2020)). Moreover, the Government "has no

obligation, under *Brady* or otherwise, to seek out . . . information like a private investigator and

valet . . . gathering evidence and delivering it to opposing counsel." *Avenatti*, 559 F. Supp. 3d at

280 (quotation marks omitted); *accord Raniere*, 384 F. Supp. 3d at 325 ("*Brady* does not require

the government to search for exculpatory material not within its possession or control.").

Here, the Government is aware of its disclosure obligations, has complied with those

obligations, and will continue to abide by those obligations. The defendants' statement that "the

government has refused to search for and produce any of this material pursuant to *Brady*," (Dkt.

51 at 1, 4), is misleading to the point of being false. The Government has already produced more

than 300,000 pages of Rule 16 materials, as well as 15 pages of substantive disclosure letters dated

August 13, 2024, and December 4, 2024 (collectively, the "Disclosure Letters"), which provide

(i) excerpts of notes and reports of witness interviews and attorney proffers identified based on the Government's understanding of potential trial defenses and defense arguments through communications with defense counsel—including the Categories they seek to compel in their motion; and (ii) the names of the corporate entities for whom the witnesses work, along with the names of each witness's respective counsel. Far from "refus[ing] to search for and produce material," as relevant to the Categories, the December 4, 2024 letter already discloses, among other things, statements provided by an uncharged co-conspirator through counsel relating to "sandwich attacks," the nature of the Victim Traders' trading activity, and methods used by cryptocurrency traders to anonymize their trading activity. In other words, to the extent that the Government identified any information in its possession or control relevant to potential trial defenses or defense arguments based on the Government's discussion with defense counsel, the Government has already produced it and will continue to produce potential defense-favorable material.

Where, as here, the Government recognizes its obligations under *Brady*, has produced potentially exculpatory material and made other, additional prophylactic disclosures, the defendant's request for an additional order pertaining to the disclosure of *Brady* material should be denied. *See, e.g.*, *United States v. Ikoli*, No. 16 Cr. 148 (AJN), 2017 WL 396681, at *3 (S.D.N.Y. Jan. 26, 2017) (denying motion to compel where "the Government represents that it recognizes its obligations under *Brady*, and that while the Government is not aware of any *Brady* material, should the Government become aware of any, it will produce it promptly").

To the extent that the defendants seek to compel the Government to affirmatively investigate and collect evidence relating to the Categories outside of what is in the Government's possession or control (which the Government has already produced through Rule 16 discovery and disclosure letters), this Court should reject such a request. *Avenatti*, 559 F. Supp. 3d at 280;

Raniere, 384 F. Supp. 3d at 325; *accord United States v. Barcelo*, 628 F. App'x 36, 38 (2d Cir. 2015) (holding that a cooperating witness was not a part of the prosecution team where he "played no role in the investigation or in determining investigation or trial strategy" and "did no more than provide information to the government and testify at trial"). Indeed, such an obligation—for which the defendants provide no authority—would be theoretically boundless and obligate the Government to scour an unknown universe of information not within the Government's control for any information that may be favorable to the defense. *Accord United States v. Hutcher*, 622 F.2d 1083, 1088 (2d Cir. 1980) ("Clearly the government cannot be required to produce that which it does not control and never possessed or inspected." (quotation marks omitted)). This is plainly not what *Brady* and its progeny require.[20] *United States v. Bonventre*, 10 Cr. 228 (LTS), 2014 WL 3673550, at *22 (S.D.N.Y. July 24, 2014) (*Brady* is "not a discovery doctrine that c[an] be used to compel the Government to gather information for the defense"), *aff'd in part*, 646 F. App'x 73 (2d Cir. 2016).

But the defendants' arguments are fatally flawed for another independently sufficient reason: because they rest on the faulty premise that the Categories constitute exculpatory information, which they do not. To start, evidence relating to the Victim Traders' trading strategies is not exculpatory evidence. *See United States v. Samuel*, 605 F. App'x 39, 40 n.1 (2d Cir. 2015) (rejecting *Brady* claim by wire fraud defendant and explaining that defendant's "allegation that his victims also engaged in fraudulent conduct was not *exculpatory* as to him" (emphasis in original)); *cf. United States v. Benson*, 548 F.2d 42, 43-44 (2d Cir. 1977) (defendant's claim that victim

---

[20] To the extent that the defendants fault the Government for "refusing" to search for potentially exculpatory information that the Government does not possess or control, (Dkt. 51 at 4), the case law makes clear that the Government is not obligated to do so.

unlawfully obtained property irrelevant to charge that defendant defrauded victim of that same

property). The defendants were not modern-day Robin Hoods entitled to steal money from the

Victim Traders even if the Victim Traders were themselves engaged in some kind of wrongdoing.

The same conclusion follows for evidence as to whether "sandwich attacks" constitute market

manipulation, which—if anything—is more akin to a defense theory, narrative, or argument

(which is not covered by *Brady*) than factual information.[21] *Cf. United States v. Bonventre*, No.

10 Cr. 228 (LTS), 2013 WL 2303726, at *29 (S.D.N.Y. May 28, 2013) (explaining that "[t]he fact

that certain knowledge could be helpful to the defense," or that the "Government's fraud case

necessarily involves evidence" that could "be consistent with defense theories," does not render

such evidence *Brady* or *Giglio* material).

The defendants' citation to the Ninth Circuit's decision in *United States v. Braunstein*, for

the proposition that evidence that the victim knew of and condoned the defendant's "gray market"

sales of its products rendered the fraud prosecution frivolous, has no application here. To start,

the issue on appeal in *Braunstein* was whether defense counsel could collect attorney's fees under

the Hyde Amendment for a frivolous prosecution. *United States v. Braunstein*, 281 F.3d 982 (9th

---

[21] Indeed, the defendants' own characterization of "sandwich attacks" as "*malicious* behavior (or at least controversial behavior)" underscores the non-factual, argumentative nature of how sandwich attacks are categorized. (Dkt. 51 at 6; *see also id.* at 8-11 (arguing at length based on unverified internet publications that sandwich attacks are "malicious")). But the fact that the defendants have a competing, defense-favorable description of sandwich attacks as "malicious market manipulation" does not render such evidence exculpatory.

Similarly, the defendants argue that evidence that the Victim Traders engaged in malicious sandwich attacks is exculpatory because it undermines the probative value of the terms "attack" or "malicious," to the extent that the Government seeks to hang its fraud theory on how third party commentators described the transaction charged in the Indictment. (Dkt. 51 at 11). Again, the exculpatory value of the way in which the defendants' actions were described by others is not immediately apparent, and it is not the case in any event that *any* information that is consistent with defense theories is *Brady* material.

Cir. 2002). The Ninth Circuit concluded that "the government's position was so obviously wrong as to be frivolous" not just because the victim "could not be deceived about practices it actively endorsed," but also because no evidence was presented to the grand jury as to any misrepresentation by the defendant. *Id.* 996-97. Here, by contrast, and as explained above, the defendants made material misrepresentations regarding the Lure Transactions and False Signature with the intent to fraudulently obtain the Victim Traders' money, and importantly, the Victim Traders did not know about the nature of the Lure Transactions or the False Signature, much less endorse them.

For similar reasons, information regarding the anonymity of the Victim Traders and actions they took to preserve their anonymity are not exculpatory in nature because such information would not tend to prove or negate the defendants' participation in the charged offenses. The defendants claim that any efforts by the Victim Traders' to conceal their identities would be exculpatory by supporting a potential defense argument that a desire for anonymity is not necessarily suggestive of criminal intent. (Dkt. 51 at 14). But the intent of the Victim Traders (or other market actors) in desiring anonymity—including after the fraudulent transaction at issue[22]— is not probative as to the *defendants*' intent in preparing for and executing the fraudulent scheme. In other words, defendants compare apples with oranges by equating the Victim Traders' use of pseudonyms (*see, e.g.*, Dkt. 51 at 13) with the defendants' concealment of their crimes by establishing multiple Ethereum validators, using shell companies, using intermediary cryptocurrency addresses, searching for cryptocurrency exchanges with limited oversight,

---

[22] It goes without saying that a crime victim who has discovered that he or she has been victimized may seek to remain anonymous for materially different reasons than an individual who committed a crime seeking to hide his or her tracks.

67

researching ways to launder cryptocurrency, and in fact using various cryptocurrency addresses, cryptocurrency swaps, and other transactions to hide their tracks.

Finally, the defendants' conjecture that information relating to the Victim Traders' desire for anonymity may also support other defenses is also unpersuasive. (*See* Dkt. 51 at 14). If, as the defendants speculate, the Victim Traders sought to remain anonymous to hide their own criminal activity or association with criminal enterprises, then the defendants may have refused to return the stolen cryptocurrency for innocent reasons. The problem with this argument, however, is that the defendants presumably know why they did not return the Victim Traders' cryptocurrency at the time that the Victim Traders made the request. *Raniere*, 384 F. Supp. 3d at 326 (explaining that the Government "has no obligation to disclose evidence if the defendant either knew or should have known of the essential facts permitting him to take advantage of any exculpatory evidence"). Moreover, the defendants' subjective motivations for not returning the Victim Traders' funds cannot logically depend on hypothetical criminal activity and criminal associations of the Victim Traders that are unknown to the defendants. At bottom, "[t]he rationale underlying *Brady* is not to supply a defendant with all the evidence in the Government's possession which might conceivably assist the preparation of his defense, but to assure that the defendant will not be denied access to exculpatory evidence only known to the Government." *Id.* (quotation marks omitted)).

Because the material falling within the scope of the Categories is not exculpatory within the meaning of *Brady* and its progeny, there is no basis to require its immediate disclosure as requested by the defendants (Dkt. 51 at 15), especially where the Government has already disclosed such material out of an abundance of caution. And to the extent that such information constitutes impeachment or so-called *Giglio* material, the Government will produce such material

pursuant to the deadline set by this Court, which is well within the timeframe that such materials are typically produced in this District.[23] *United States v. Coppa*, 267 F.3d 132, 146 (2d Cir. 2001) ("[A]s a general rule, *Brady* and its progeny do not require immediate disclosure of all exculpatory and impeachment material upon request by a defendant."). The defendants' motion should be denied.

IV.   The Motion for a Bill of Particulars Should Be Denied

Finally, the defendants seek a bill of particulars identifying the three Victim Traders referenced in the Indictment. (Dkt. 55). The motion should be denied as an impermissible attempt to compel the Government to disclose in advance of trial the potential witnesses the Government may call at trial.

A bill of particulars "is not a general investigative tool, a discovery device or a means to compel the government to disclose evidence *or witnesses* to be offered prior to trial." *United States v. Gibson*, 175 F. Supp. 2d 532, 537 (S.D.N.Y. 2001) (emphasis added); *see United States v. Martinez*, 22 Cr. 251 (LJL), 2023 WL 2403134, at *1 (S.D.N.Y. Mar. 8, 2023) (same). The proper purpose of a bill of particulars is "to provide a defendant with information about the details of the

---

[23] As the Court knows, typically in this District, the Government confirms that it will produce Jencks Act material and impeachment material reasonably in advance of trial. *See, e.g.*, *United States v. Wey*, No. 15 Cr. 611 (AJN), 2017 WL 237651, at *23 (S.D.N.Y. Jan. 18, 2017) ("[I]t is a widely recognized customary practice in this District that *Giglio* material is turned over at the same time as material under the Jencks Act . . . . Both types of material are typically produced a week or two before the start of trial, depending on the complexity of the case."); *United States v. Bankman-Fried*, 22 Cr. 673 (LAK) (Jencks Act material produced three-and-a-half weeks before trial); *United States v. Ulbricht*, No. 14 Cr. 68 (KBF) (Jencks Act material produced one week before trial); *United States v. Tagliaferri*, No. 13 Cr. 115 (RA) (Jencks Act material produced seventeen days before trial); *United States v. Costanza*, No. 12 Cr. 725 (KMW) (Jencks Act material produced two weeks before trial); *United States v. Whitman*, No. 12 Cr. 125 (JSR) (Jencks Act material produced two weeks before trial); *United States v. Silver*, No. 15 Cr. 93 (VEC) (Jencks Act material produced approximately three weeks before trial); *United States v. Gupta*, No. 11 Cr. 907 (JSR) (Jencks Act material produced three weeks before trial).

charge against him if this is *necessary* to the preparation of his defense, and to avoid prejudicial surprise at trial." *United States v. Torres*, 901 F.2d 205, 234 (2d Cir. 1990) (emphasis added), *abrogated on other grounds by United States v. Marcus*, 628 F.3d 36, 41 (2d Cir. 2010); *see also United States v. Leonelli*, 428 F. Supp. 880, 882 (S.D.N.Y. 1977); *United States v. Mahabub*, 13 Cr. 908 (AJN), 2014 WL 4243657, at *2 (S.D.N.Y. Aug. 26, 2014) ("The purpose of a bill of particulars is to ensure that a defendant has the information necessary to prepare a defense, not to turn over all information that would aid the defendant."). Accordingly, a bill of particulars is required "only where the charges of the indictment are so general that they do not advise the defendant of the specific acts of which he is accused." *United States v. Walsh*, 194 F.3d 37, 47 (2d Cir. 1999).

Factors that courts weigh when considering whether a bill of particulars is necessary include the Indictment's text, as well as discovery and other information that has and will be provided to the defendant concerning the Government's allegations. *See United States v. Bortnovsky*, 820 F.2d 572, 574 (2d Cir. 1987); *see also, e.g.*, *United States v. Brewster*, 19 Cr. 833 (SHS), 2021 WL 3423521, at *2 (S.D.N.Y. Aug. 5, 2021) ("Because the defense has received, and will continue to receive, information from the government that will assist them in preparing their defense, the motion to compel a bill of particulars as to all defendants is denied without prejudice.").

Here, the 19-page speaking Indictment, supplemented by well-indexed and searchable Rule 16 discovery, provides the defendants with more than enough notice about the charged crimes and ample information to adequately prepare their defense. *See Bortnovsky*, 820 F.2d at 574; *see also United States v. Rigas*, 258 F. Supp. 2d 299, 305 (S.D.N.Y. 2003) (explaining that the law does not "allow [a] Defendant[] to use the vastness or complexity of the alleged conspiracy and its

attendant documentary evidence as a sword against the government, when the Indictment, discovery, and other information provided by the government adequately notify [the] Defendant[] of the charges against [him]"). Indeed, the charges in this case rest on a single set of fraudulent transactions that netted the defendants an approximately $25 million in fraud proceeds, so there is minimal danger—if any at all—of prejudicial surprise at trial as to which transaction is at issue in this case. The Indictment also details the date of the fraudulent transaction and the approximate timeframe of the defendants' participation in the fraud scheme, the means and methods that the defendants used to plan, execute, and conceal the fraud, the number of victims who were defrauded, and the various transactions and accounts that the defendants used to obscure the provenance of the fraud proceeds.

The allegations in the Indictment, along with multiple search warrant applications produced as part of more than 300,000 pages of Rule 16 discovery and two substantive disclosure letters,[24] "sufficiently apprise[] [the defendants] of the nature and details of the charges against [them] that a bill of particulars is not warranted." *United States v. Dupigny*, 18 Cr. 528 (JMF), 2019 WL 2327697, at *2 (S.D.N.Y. May 30, 2019); *accord United States v. L.*, 16 Cr. 676 (LGS), 2017 WL 1435746, at *2 (S.D.N.Y. Apr. 21, 2017) (denying bill of particulars request where the "Government . . . represents that it provided search warrant affidavits that describe its investigation and evidence"). The Indictment, well-labeled discovery, and these disclosures more than meet the Government's obligations, and—as is routine—the Government here plans to disclose a witness

---

[24] As noted in Section III, the Disclosure Letters provide excerpts of witness statements and factual proffers from counsel for the witnesses, which were identified based on the Government's understanding of defense theories and arguments from discussions with defendants' counsel. Notably, the Disclosure Letters disclosed the business entity associated with Victim Trader-1, along with the name of counsel for Victim Trader-1. As to Victim Traders-2 and -3, the Government has already disclosed any information in the Government's possession or control.

71

list and Section 3500 material sufficiently in advance of trial for the defense to adequately prepare. *See United States v. Trippe*, 171 F. Supp. 2d 230, 240 (S.D.N.Y. 2001).

None of the defendants' contentions as to the purported need to learn the Victim Traders' identities has merit—especially as to Victim Trader-1, for whom the Government has already disclosed the associated business entity and counsel. The defendants first contend that without knowledge of the identities of the Victim Traders, the defendants' ability to issue subpoenas pursuant to Federal Rule of Criminal Procedure 17 (including subpoenas to produce documents prior to trial) would be hindered.[25] Even assuming there is a proper basis for a Rule 17 subpoena— a basis that has yet to be articulated—it is hard to imagine how the defendants are hindered in any way since they have the ability to serve Victim-1's counsel. What this argument really seeks is "to use the victims' identities to conduct discovery, which is not the purpose of a bill of particulars." *United States v. Kelly*, 2020 WL 473613, at *2 (E.D.N.Y. Jan. 29, 2020) (rejecting request for bill of particulars based on defense argument that "it is 'impossible to interview witnesses' or 'to search for records' without the identifying information"); *accord Dupigny*, 2019 WL 2327697, at *2 (rejecting defense request for particulars, including identities of three victims

---

[25] There is also reason to believe that the Rule 17 subpoenas would be improper even if the Victim Traders' identities were disclosed, which further underscores the lack of justification for the defendants' request for a bill of particulars. Under well-established law, discovery in criminal cases is not properly conducted through Rule 17 subpoenas, which "[are] not intended as a means of discovery." *United States v. Purin*, 486 F.2d 1363, 1368 (2d Cir. 1973); *see also Bowman Dairy Co. v. United States*, 341 U.S. 214, 219-20 (1951). But the defendants' request for a bill of particulars reveals that they wish to obtain the identities of the Victim Traders so that they can serve Rule 17 subpoenas as a discovery device, as opposed to obtaining specific, relevant, and admissible materials for use at trial. *United States v. Nixon*, 418 683, 699-700 (1974) (outlining the strict requirements for issuance of Rule 17 subpoenas). Rule 17 plainly cannot be used "to obtain leads as to the existence of additional documentary evidence or to seek information relating to the defendant's case," because "[t]his type of discovery, permissible under the Federal Rules of Civil Procedure, has not been authorized for criminal trials." *United States v. Gross*, 24 F.R.D. 138, 141 (S.D.N.Y. 1959).

in sex trafficking case, to enable defendant to "locate witnesses" and "perform a meaningful investigation").

Next, the defendants' contention that the identification of the victims is needed to determine what overall defenses are available is conclusory and sheds no light on *why* or *how* the identification of these victims would be necessary to the defendants' preparation for trial. Relatedly, the defendants' claim that how the Government defines the victims—whether as individuals, entities, or a piece of technology—may impact the potential factual or legal defenses available fails to explain with any specificity what exactly that impact may be, much less why an order for the Government to provide the identities of the Victim Traders would provide the defendants any clarity as to how the victims are defined. The closest that defendants come to any explanation of why the victims' *identities* in particular would be necessary for them to prepare for trial is that the identities would allow them to determine whether there are victim-specific defenses available—for example, by defining the relevant rules and protocols of the network. This argument, too, crumbles with scrutiny. For one thing, defendants again fail to explain how knowing the names of the Victim Traders would, standing alone, enable them to determine what victim-specific defenses are available. If anything, this argument simply veils the actual purpose of the defendants' request: to "use the victims' identities to conduct discovery, which is not the purpose of a bill of particulars." *Kelly*, 2020 WL 473613, at *2. Moreover, information regarding the rules and protocols of the network has already been disclosed to the defendants in the Government's disclosure letters, which include excerpts of witness statements from representatives of the relay and the research organization that designed the MEV-Boost software, whose identities and counsel information were also disclosed to the defendants. With respect to each of these requests, while more information might be considered "helpful," the "ultimate test

must be whether the information sought is necessary." *United States v. Mitlof*, 165 F. Supp. 2d 558, 569 (S.D.N.Y. 2001). Defendants fail to make that showing here.

The cases that the defendants cite for the proposition that courts "often" order the Government to identify victims are also distinguishable and do not support the defense request for a bill of particulars here. (Dkt. 55 at 2-3). For example, unlike in *Davidoff*, where the defendant sought the identities of victims of *uncharged* acts of racketeering, *United States v. Davidoff*, 845 F.2d 1151, 1152 (2d Cir. 1998), the defendants here seek the identities of victims of the charged offenses—offenses that are outlined in detail in the Indictment, *see United States v. Cordones*, 11 Cr. 205 (AKH), 2022 WL 815229, at *8 (S.D.N.Y. Mar. 17, 2022) ("Courts routinely deny motions for bills of particulars where, as here, the charging document is a speaking indictment."). Similarly, *Solnin* is readily distinguishable because the Government in that case had previously "expressed no objection to disclosing to the Defense counsel the identities of the John Doe victims."[26] *United States v. Solnin*, 81 F. Supp. 3d 193, 209 (E.D.N.Y. 2015). The decisions in *Raymond* and *Zandstra* do not support the defendant's contentions, either. In *Raymond*, the court ordered a bill of particulars because "[t]he sheer number of alleged victims for just one criminal defendant poses a relatively unique challenge" to the defendant which "may well [leave defendant] guessing as to the precise identity of which individual corresponds to a particular alleged victim," where the defendant was charged with "abus[ing] as many as twenty-six women across three countries and seven years." *United States v. Raymond*, 21 Cr. 380 (CKK), 2023 WL 6294178, at

---

[26] The court in *Solnin* independently found that disclosure of the John Doe victims' identities was warranted without further explanation. *Solnin*, 81 F. Supp. 3d at 209. Similarly, the court in *Johnson* ordered the Government to disclose the identities of victims without further explanation. *United States v. Johnson*, 21 F. Supp. 2d 329, 340 (S.D.N.Y. 1998). Accordingly, the persuasive force of these cases is limited.

*4 (D.D.C. Sept. 27, 2023). And in *Zandstra*, the court ordered a bill of particulars where the "discovery provided identifies twelve possible victims" and further "suggests that dozens of other individuals may have been solicited." *United States v. Zandstra*, 00 Cr. 209 (RWS), 2000 WL 1368050, at 6 & n.3 (S.D.N.Y. Sept. 20, 2020). Here, by contrast, the charged scheme involves one fraudulent transaction and three victims—the nature of which has been made amply clear through the Indictment, discovery productions, and disclosure letters. The defendants' motion for a bill of particulars is nothing more than an attempt to seek premature disclosure of victim-witness identities far in advance of trial and should be denied.

CONCLUSION

For the reasons set forth above, the defendants' motions should be denied.

Respectfully submitted,

MATTHEW PODOLSKY
Chief Counsel to the
Acting United States Attorney
Attorney for the United States,
Acting Under Authority Conferred by
28 U.S.C. § 515

By: /s/ Danielle Kudla
    Rushmi Bhaskaran
    Jerry Fang
    Danielle Kudla
    Assistant United States Attorneys
    212-637-2439 / 2584 / 2304

Dated: January 17, 2025
        New York, New York